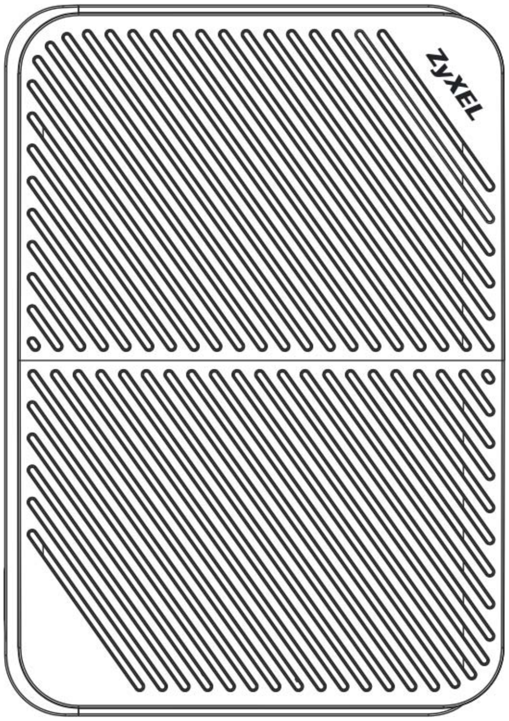
P-660HN-51

802.11n Wireless ADSL2+ 4-port Gateway

User's Guide



Default Login Details

IP Address	http://192.168.1.1
User Name	admin
Password	1234

Firmware Version 1.10
Edition 1, 11/2010

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Support Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

Documentation Feedback

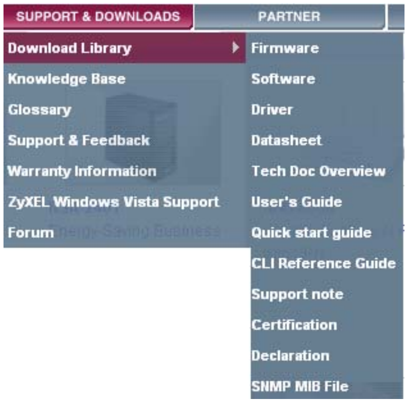
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Disclaimer

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

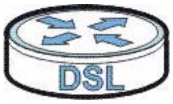
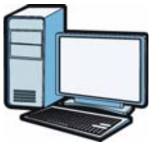
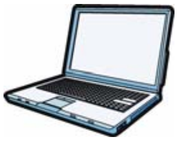
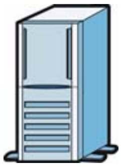
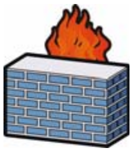
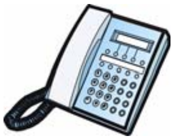
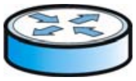
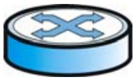
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-660HN-51 may be referred to as the "ZyXEL Device", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User’s Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device  	Computer 	Notebook computer 
Server 	Firewall 	Telephone 
Router 	Switch 	

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Contents Overview

User’s Guide 19

Introduction 21
The Web Configurator 27
Network Map and Status Screens 35
Tutorials 41

Technical Reference 61

Broadband 63
Wireless 77
Home Networking 113
Network Address Translation (NAT) 133
MAC Filter 151
Firewall 153
Remote Management 163
Certificates 165
IPSec 177
Parental Control 197
Routing 201
Dynamic DNS Setup 205
Quality of Service (QoS) 211
TR-069 Client 231
Time Settings 235
Scheduler Rules 239
Policy Forwarding 241
Logs 245
Introduction to the ARP Table 251
Traffic Status 253
Users Configuration 257
Logs Setting 261
Firmware Upgrade 265
Configuration 267
Diagnostic 271
Troubleshooting 275
Product Specifications 281

Table of Contents

About This User's Guide 3

Document Conventions 5

Safety Warnings 7

Contents Overview 9

Table of Contents 11

Part I: User’s Guide 19

Chapter 1
Introduction 21

1.1 Overview 21
1.2 Ways to Manage the ZyXEL Device 21
1.3 Good Habits for Managing the ZyXEL Device 22
1.4 Applications for the ZyXEL Device 22
1.4.1 Internet Access 22
1.5 Wireless Access 23
1.5.1 Using the WLAN/WPS Button 23
1.6 LEDs (Lights) 25
1.7 The RESET Button 26
1.7.1 Using the RESET Button 26

Chapter 2
The Web Configurator 27

2.1 Overview 27
2.1.1 Accessing the Web Configurator 27
2.2 The Web Configurator Layout 29
2.2.1 Title Bar 30
2.2.2 Main Window 30
2.2.3 Navigation Panel 30

Chapter 3
Network Map and Status Screens 35

3.1 Overview 35
3.2 The Network Map Screen 35

3.3 The Status Screen 37

Chapter 4
Tutorials 41

4.1 Overview 41
4.2 Setting Up Your DSL Connection Using PPPoE 41
4.3 Setting Up a Secure Wireless Network 44
4.3.1 Configuring the Wireless Network Settings 44
4.3.2 Using WPS 46
4.3.3 Without WPS 51
4.4 Setting Up Multiple Wireless Groups 52
4.5 Configuring Static Route for Routing to Another Network 55
4.6 Access the ZyXEL Device Using DDNS 58
4.6.1 Registering a DDNS Account on www.dyndns.org 58
4.6.2 Configuring DDNS on Your ZyXEL Device 59
4.6.3 Testing the DDNS Setting 59

Part II: Technical Reference 61

Chapter 5
Broadband 63

5.1 Overview 63
5.1.1 What You Need to Know 63
5.1.2 Before You Begin 64
5.2 The Broadband Screen 65
5.2.1 Add/Edit Broadband 66
5.3 Technical Reference 73
5.3.1 Encapsulation 73
5.3.2 Multiplexing 74
5.3.3 VPI and VCI 74
5.3.4 IP Address Assignment 74
5.3.5 NAT 75
5.4 Traffic Shaping 75
5.4.1 ATM Traffic Classes 76

Chapter 6
Wireless 77

6.1 Overview 77
6.1.1 What You Can Do in this Chapter 77
6.1.2 What You Need to Know 78
6.2 The General Screen 78

6.2.1 No Security 81
6.2.2 Basic (WEP Encryption) 81
6.2.3 More Secure (WPA(2)-PSK) 83
6.2.4 WPA(2) Authentication 84
6.3 The More AP Screen 86
6.3.1 Edit More AP 87
6.4 MAC Authentication 88
6.5 The WPS Screen 90
6.6 The WMM Screen 91
6.7 The WDS Screen 92
6.7.1 WDS Scan 94
6.8 The Wireless Others Screen 95
6.9 Technical Reference 96
6.9.1 Wireless Network Overview 96
6.9.2 Additional Wireless Terms 98
6.9.3 Wireless Security Overview 99
6.9.4 Signal Problems 102
6.9.5 BSS 102
6.9.6 MBSSID 103
6.9.7 Wireless Distribution System (WDS) 104
6.9.8 WiFi Protected Setup (WPS) 104
6.9.9 Preamble Type 111

Chapter 7
Home Networking 113

7.1 Overview 113
7.1.1 What You Can Do in this Chapter 113
7.1.2 What You Need To Know 114
7.1.3 Before You Begin 115
7.2 The LAN Setup Screen 116
7.3 The Static DHCP Screen 118
7.4 The UPnP Screen 119
7.5 Installing UPnP in Windows Example 120
7.6 Using UPnP in Windows XP Example 123
7.7 Technical Reference 128
7.7.1 LANs, WANs and the ZyXEL Device 129
7.7.2 DHCP Setup 129
7.7.3 DNS Server Addresses 129
7.7.4 LAN TCP/IP 130

Chapter 8
Network Address Translation (NAT) 133

8.1 Overview 133

8.1.1 What You Can Do in this Chapter 133
8.1.2 What You Need To Know 133
8.2 The Port Forwarding Screen 134
8.2.1 Add/Edit Port Forwarding 136
8.3 The Applications Screen 137
8.3.1 Add New Application 138
8.4 The Port Triggering Screen 139
8.4.1 Add/Edit Port Triggering Rule 141
8.5 The DMZ Screen 143
8.6 The ALG Screen 144
8.7 The Sessions Screen 144
8.8 Technical Reference 145
8.8.1 NAT Definitions 145
8.8.2 What NAT Does 146
8.8.3 How NAT Works 147
8.8.4 NAT Application 148

Chapter 9
MAC Filter 151

9.1 Overview 151
9.2 The MAC Filter Screen 151

Chapter 10
Firewall 153

10.1 Overview 153
10.1.1 What You Can Do in this Chapter 153
10.1.2 What You Need to Know 154
10.2 The Firewall Screen 155
10.3 The Protocol Screen 155
10.3.1 Add a Protocol 156
10.4 The Access Control Screen 157
10.4.1 Add/Edit an ACL Rule 159

Chapter 11
Remote Management 163

11.1 Overview 163
11.2 The Service Control Screen 163

Chapter 12
Certificates 165

12.1 Overview 165
12.1.1 What You Can Do in this Chapter 165
12.2 What You Need to Know 165

12.3 The Local Certificates Screen 166
12.3.1 Create Certificate Request 167
12.3.2 Import Certificate 168
12.3.3 Certificate Details 170
12.4 The Trusted CA Screen 172
12.4.1 View Trusted CA Certificate 173
12.4.2 Import Trusted CA Certificate 174

Chapter 13
IPSec 177

13.1 Overview 177
13.1.1 What You Can Do in this Chapter 177
13.1.2 What You Need to Know 178
13.2 The IPSec Settings Screen 179
13.2.1 Add/Edit IPSec Setting 180
13.2.2 Configuring Manual Key 185
13.3 The IPSec Status Screen 188
13.4 Technical Reference 188
13.4.1 IPSec Architecture 189
13.4.2 Encapsulation 190
13.4.3 IKE Phases 191
13.4.4 Negotiation Mode 192
13.4.5 IPSec and NAT 192
13.4.6 VPN, NAT, and NAT Traversal 193
13.4.7 ID Type and Content 194
13.4.8 Pre-Shared Key 195
13.4.9 Diffie-Hellman (DH) Key Groups 196

Chapter 14
Parental Control 197

14.1 Overview 197
14.2 The Parental Control Screen 197
14.2.1 Add/Edit Parental Control Rule 198

Chapter 15
Routing 201

15.1 Overview 201
15.2 The Routing Screen 202
15.2.1 Add/Edit Static Route 203

Chapter 16
Dynamic DNS Setup 205

16.1 Overview 205

16.1.1 What You Can Do in this Chapter 206
16.1.2 What You Need To Know 207
16.2 The DNS Entry Screen 207
16.2.1 Add/Edit DNS Entry 208
16.3 The Dynamic DNS Screen 208

Chapter 17
Quality of Service (QoS) 211

17.1 Overview 211
17.1.1 What You Can Do in this Chapter 211
17.2 What You Need to Know 212
17.3 The Quality of Service General Screen 213
17.4 The Queue Setup Screen 214
17.4.1 Adding a QoS Queue 215
17.5 The Class Setup Screen 216
17.5.1 Add/Edit QoS Class 218
17.6 The QoS Policer Setup Screen 222
17.6.1 Add/Edit a QoS Policer 223
17.7 The QoS Monitor Screen 224
17.8 Technical Reference 225

Chapter 18
TR-069 Client 231

18.1 Overview 231
18.2 The TR-069 Clients Screen 231

Chapter 19
Time Settings 235

19.1 Overview 235
19.2 The Time Setting Screen 235

Chapter 20
Scheduler Rules 239

20.1 Overview 239
20.2 The Scheduler Rules Screen 239
20.2.1 Add/Edit a Schedule 240

Chapter 21
Policy Forwarding 241

21.1 Overview 241
21.2 The Policy Forwarding Screen 241
21.2.1 Add/Edit Policy Forwarding 242

Chapter 22
Logs 245

22.1 Overview 245
22.1.1 What You Can Do in this Chapter 245
22.1.2 What You Need To Know 245
22.2 The System Log Screen 246
22.3 The Security Log Screen 248

Chapter 23
Introduction to the ARP Table 251

23.1 Overview 251
23.1.1 How ARP Works 251
23.2 ARP Table Screen 252

Chapter 24
Traffic Status 253

24.1 Overview 253
24.1.1 What You Can Do in this Chapter 253
24.2 The WAN Status Screen 254
24.3 The LAN Status Screen 255

Chapter 25
Users Configuration 257

25.1 Overview 257
25.2 The Users Configuration Screen 257
25.2.1 Add/Edit a Users Account 258
25.2.2 Types of Accounts 259

Chapter 26
Logs Setting 261

26.1 Overview 261
26.2 The Log Settings Screen 261

Chapter 27
Firmware Upgrade 265

27.1 Overview 265
27.2 The Firmware Screen 265

Chapter 28
Configuration 267

28.1 Overview 267
28.2 The Configuration Screen 267
28.3 The Reboot Screen 270

Chapter 29
Diagnostic...271

29.1 Overview 271
29.1.1 What You Can Do in this Chapter 271
29.2 The Ping & TraceRoute & NsLookup Screen 271
29.3 The OAM Ping Test Screen 272

Chapter 30
Troubleshooting...275

30.1 Power, Hardware Connections, and LEDs 275
30.2 ZyXEL Device Access and Login 276
30.3 Internet Access 278
30.4 Wireless Internet Access 279

Chapter 31
Product Specifications...281

31.1 Hardware Specifications 281
31.2 Firmware Specifications 281
31.3 Wireless Features 284

Appendix A Setting up Your Computer’s IP Address..287

Appendix B Pop-up Windows, JavaScript and Java Permissions....................... 311

Appendix C IP Addresses and Subnetting 321

Appendix D Wireless LANs 331

Appendix E Services 347

Appendix F Open Software Announcements 351

Appendix G Legal Information...363

Index...367

PART I

User's Guide

1

Introduction

1.1 Overview

The P-660HN-51 is an ADSL2+ router. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access. The P-660HN-51 is also a complete security solution with a robust firewall and content filtering.

Please refer to the following description of the product name format.

- "H" denotes an integrated 4-port hub (switch).
- "N" denotes 802.11n draft 2.0. The "N" models support 802.11n wireless connection mode.
- Models ending in "1", for example P-660HN-51, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service).

Only use firmware for your ZyXEL Device's specific model. Refer to the label on the bottom of your ZyXEL Device.

Note: All screens displayed in this user's guide are from the P-660HN-51 model.

See the product specifications for a full list of features.

1.2 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.
- TR-069. This is an auto-configuration server used to remotely configure your device.

1.3 Good Habits for Managing the ZyXEL Device

Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

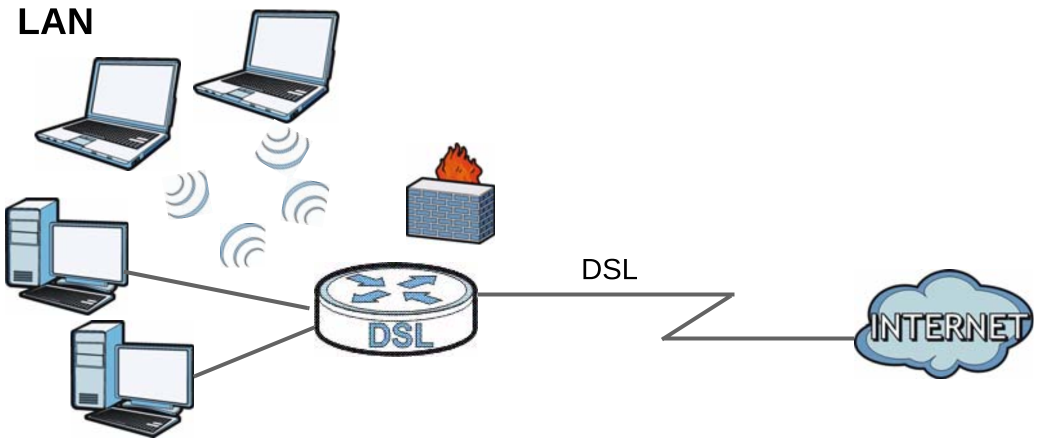
1.4 Applications for the ZyXEL Device

Here are some example uses for which the ZyXEL Device is well suited.

1.4.1 Internet Access

Your ZyXEL Device provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. Computers can connect to the ZyXEL Device's LAN ports (or wirelessly).

Figure 1 ZyXEL Device's Router Features



You can also configure firewall and filtering feature on the ZyXEL Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

Use the filtering feature to block access to specific web sites or Internet applications such as MSN or Yahoo Messanger. You can also configure IP/MAC filtering rules for incoming or outgoing traffic.

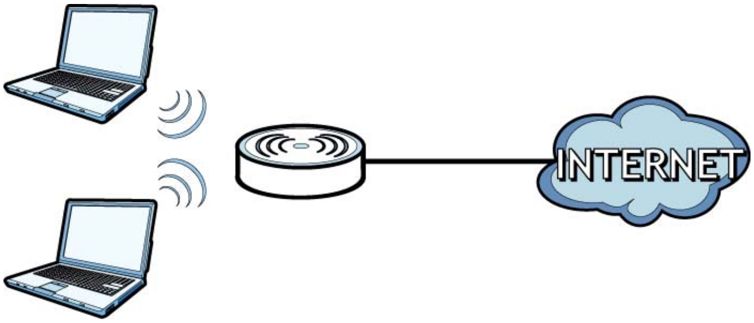
Use QoS to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers. For example, you could make sure that the ZyXEL Device gives voice over Internet calls high priority, and/or limit bandwidth devoted to the boss's excessive file downloading.

1.5 Wireless Access

The ZyXEL Device is a wireless Access Point (AP) for wireless clients, such as notebook computers or PDAs and iPads. It allows them to connect to the Internet without having to rely on inconvenient Ethernet cables.

You can configure your wireless network in either the built-in Web Configurator, or using the WPS button.

Figure 2 Wireless Access Example



1.5.1 Using the WLAN/WPS Button

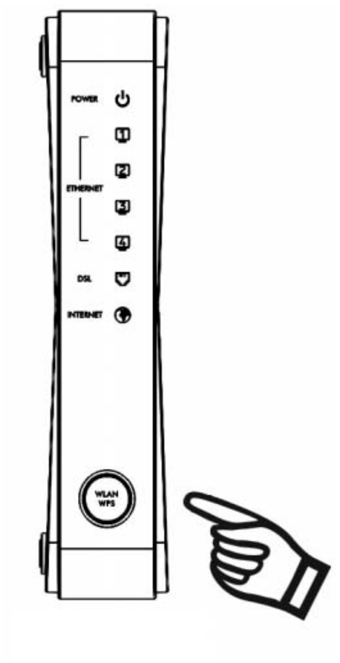
By default, the wireless network is turned on. If it is turned off, simply press the **WLAN/WPS** button in front of the ZyXEL Device for 1 second. Once the **WLAN/WPS** LED turns green, the wireless network is active.

You can also use the **WPS/WLAN** button to quickly set up a secure wireless connection between the ZyXEL Device and a WPS-compatible client by adding one device at a time.

To activate WPS:

1 Make sure the **POWER** LED is on and not blinking.

2 Press the **WLAN/WPS** button for five to ten seconds and release it.



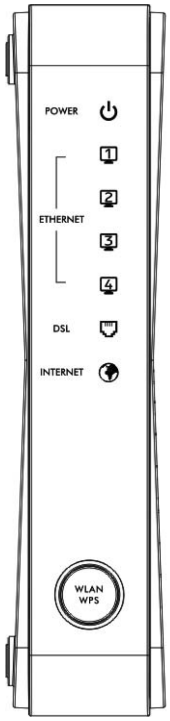
3 Press the WPS button on another WPS-enabled device within range of the ZyXEL Device. The **WPS/WLAN** LED should flash while the ZyXEL Device sets up a WPS connection with the other wireless device.

4 Once the connection is successfully made, the **WPS/WLAN** LED shines green.

1.6 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 3 LEDs



None of the LEDs are on if the ZyXEL Device is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power and ready for use.
		Blinking	The ZyXEL Device is self-testing.
	Red	On	The ZyXEL Device detected an error while self-testing, or there is a device malfunction.
		Off	The ZyXEL Device is not receiving power.
LAN 1-4	Green	On	The ZyXEL Device has an Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The ZyXEL Device is sending/receiving data to/from the LAN.
		Off	The ZyXEL Device does not have an Ethernet connection with the LAN.
WPS/ WLAN	Green	On	The wireless network is activated.
		Blinking	The ZyXEL Device is communicating with other wireless clients.
	Orange	Blinking	The ZyXEL Device is setting up a WPS connection.
		Off	The wireless network is not activated.

Table 1 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
DSL	Green	On	The DSL line is up.
		Blinking	The ZyXEL Device is initializing the DSL line.
		Off	The DSL line is down.
INTERNET	Green	On	The ZyXEL Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The ZyXEL Device is sending or receiving IP traffic.
	Red	On	The ZyXEL Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	The ZyXEL Device does not have an IP connection.

Refer to the Quick Start Guide for information on hardware connections.

1.7 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “1234”.

1.7.1 Using the RESET Button

1 Make sure the **POWER** LED is on (not blinking).

2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

2

The Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions or Mozilla Firefox 3 and later versions or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

See Appendix B on page 311 if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

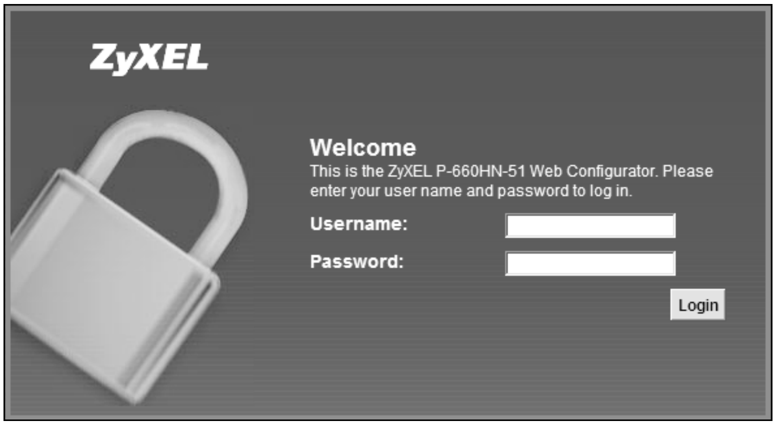
1 Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).

2 Launch your web browser.

3 Type "192.168.1.1" as the URL.

4 A password screen displays. To access the administrative web configurator and manage the ZyXEL Device, type the default username **admin** and password **1234** in the password screen and click **Login**. If you have changed the password, enter your password and click **Login**. For security reasons, you will be temporarily denied access to the ZyXEL Device for a period of time (15 minutes by default) if you have entered the incorrect username and password for a certain number of times (three times by default).

Figure 4 Password Screen



Welcome

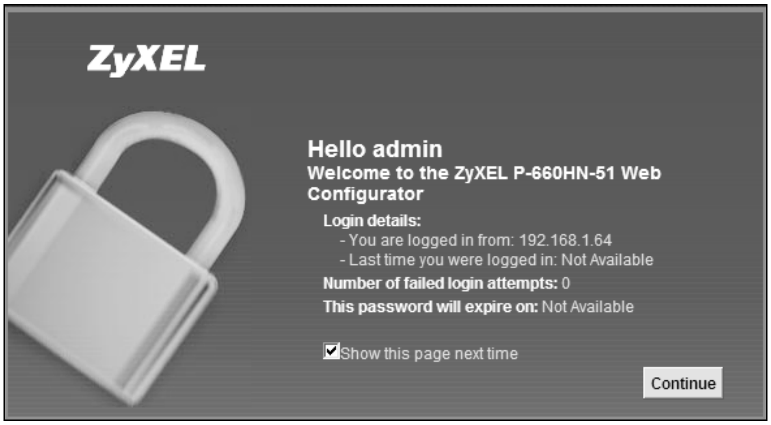
This is the ZyXEL P-660HN-51 Web Configurator. Please enter your user name and password to log in.

Username:

Password:

5 A welcome screen appears showing a summary of your last login, such as the time, number of failed login attempts, and when the password expires. It also shows if you are logged on from an IP address. Select **Show this page next time** to see the welcome screen on your next login. Otherwise, deselect it. Click **Continue**.

Figure 5 Welcome Screen



Hello admin

Welcome to the ZyXEL P-660HN-51 Web Configurator

Login details:

- You are logged in from: 192.168.1.64
- Last time you were logged in: Not Available

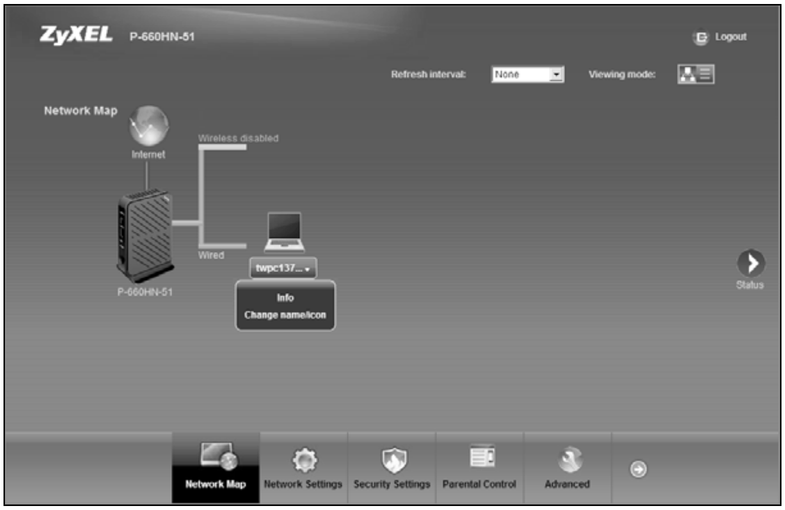
Number of failed login attempts: 0

This password will expire on: Not Available

☑ Show this page next time

6 The **Network Map** page appears.

Figure 6 Network Map

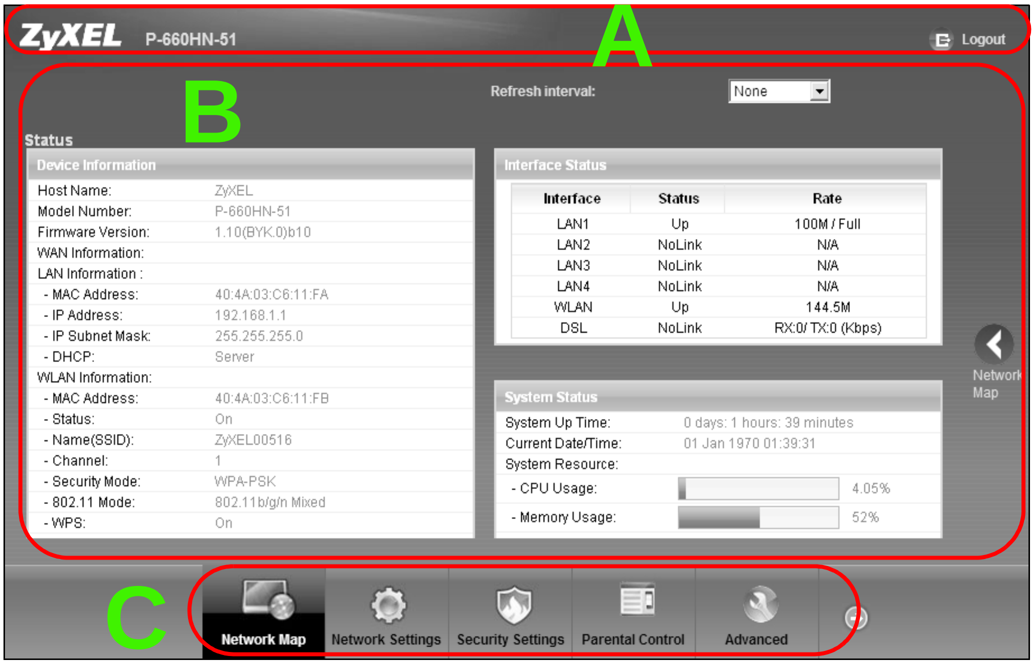


Note: For security reasons, the ZyXEL Device automatically logs you out if you do not use the web configurator for ten minutes (default). If this happens, log in again.

7 Click **Status** to display the **Status** screen, where you can view the ZyXEL Device's interface and system information.

2.2 The Web Configurator Layout

Figure 7 The Web Configurator Layout



Device Information

Host Name:	ZyXEL
Model Number:	P-660HN-51
Firmware Version:	1.10(BYK.0)b10
WAN Information:	
LAN Information :	
- MAC Address:	40:4A:03:C6:11:FA
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information:	
- MAC Address:	40:4A:03:C6:11:FB
- Status:	On
- Name(SSID):	ZyXEL00516
- Channel:	1
- Security Mode:	WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	On

Interface Status

Interface	Status	Rate
LAN1	Up	100M / Full
LAN2	NoLink	N/A
LAN3	NoLink	N/A
LAN4	NoLink	N/A
WLAN	Up	144.5M
DSL	NoLink	RX:0/ TX:0 (Kbps)

System Status

System Up Time:	0 days: 1 hours: 39 minutes
Current Date/Time:	01 Jan 1970 01:39:31
System Resource:	
- CPU Usage:	4.05%
- Memory Usage:	52%

As illustrated above, the web configurator layout is divided into these parts:

- **A** - title bar
- **B** - main window
- **C** - navigation panel

2.2.1 Title Bar

The title bar provides some icons in the upper right corner.

Click this icon to log out of the web configurator.

2.2.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

After you click **Status** on the **Network Map** page, the **Status** screen is displayed. See Chapter 3 on page 37 for more information about the **Status** screen.

2.2.3 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyXEL Device features. The following tables describe each menu item.2

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Network Map		This screen shows the network status of the ZyXEL Device and computers/devices connected to it.
Network Settings		
Broadband	Broadband	Use this screen to view and configure ISP parameters, WAN IP address assignment, and other advanced properties. You can also add new WAN connections.

Table 2 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Wireless	General	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	More AP	Use this screen to configure multiple BSSs on the ZyXEL Device.
	MAC Authentication	Use this screen to block or allow wireless traffic from wireless devices of certain SSIDs and MAC addresses to the ZyXEL Device.
	WPS	Use this screen to configure and view your WPS (Wi-Fi Protected Setup) settings.
	WMM	Use this screen to enable or disable Wi-Fi MultiMedia (WMM).
	WDS	Use this screen to set up Wireless Distribution System (WDS) links to other access points.
	Others	Use this screen to configure advanced wireless settings.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to enable the UPnP function.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Applications	Use this screen to configure servers behind the ZyXEL Device.
	Port Triggering	Use this screen to change your ZyXEL Device’s port triggering settings.
	DMZ	Use this screen to configure a default server which receives packets from ports that are not specified in the **Port Forwarding** screen.
	ALG	Use this screen to enable or disable SIP ALG.
	Sessions	Use this screen to limit the number of NAT sessions all clients can establish.
Security Settings		
MAC Filter	MAC Filter	Use this screen to configure the ZyXEL Device to give exclusive access to specific devices or exclude specific devices from accessing the ZyXEL Device.
Firewall	General	Use this screen to configure the security level of your firewall.
	Protocol	Use this screen to add or remove predefined Internet services and configure firewall rules.
	Access Control	Use this screen to enable specific traffic directions for network services.
Remote MGMT	Remote MGMT	Use this screen to enable specific traffic directions for network services.
Certificates	Local Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CA	Use this screen to view and manage the list of the trusted CAs.
IPSec VPN	Status	Use this screen to view the status of IPSec tunnels.
	Settings	Use this screen to add and configure IPSec tunnels.

Table 2 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Parental Control	Parental Control	Use this screen to block web sites with the specific URL.
Advanced		
Routing	Routing	Use this screen to view and set up static routes on the ZyXEL Device.
DNS Setting	DNS Entry	Use this screen to view and configure DNS entries.
	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
QoS	General	Use this screen to enable QoS and traffic prioritizing. You can also configure the QoS rules and actions.
	Queue Setup	Use this screen to configure QoS queues.
	Class Setup	Use this screen to define a classifier.
	Policer Setup	Use these screens to configure QoS policers.
	Monitor	Use this screen to view QoS packets statistics.
TR-069 Client	TR-069 Client	Use this screen to configure the ZyXEL Device to be managed by an Auto Configuration Server (ACS).
Time Setting	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Scheduler Rules	Scheduler Rules	Use this screen to configure the days and times when a configured restriction (such as parental control) is enforced.
Policy Forwarding	Policy Forwarding	Use this screen to configure policy routing on the ZyXEL Device.
System Monitor		
ARP Table	ARP Table	Use this screen to view the ARP table. It displays the IP and MAC address of each DHCP connection.
Log	System Log	Use this screen to view the status of events that occurred to the ZyXEL Device. You can export or e-mail the logs.
	Security Log	Use this screen to view the login record of the ZyXEL Device. You can export or e-mail the logs.
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the ZyXEL Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the ZyXEL Device.
Maintenance		
Users Configuration	Users Configuration	Use this screen to add and configure user accounts on the ZyXEL Device.
Logs Setting	Logs Setting	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your device.
Configuration	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
Reboot	Reboot	Use this screen to reboot the ZyXEL Device without turning the power off.

Table 2 Navigation Panel Summary (continued)

LINK	TAB	FUNCTION
Diagnostic	Ping & TraceRoute & NsLookup	Use this screen to identify problems with the DSL connection. You can use Ping, TraceRoute, or Nslookup to help you identify problems.
	OAM Ping	Use this screen to send an ATM OAM (Operation, Administration and Maintenance) packet to verify the connectivity of a specific PVC.

3

Network Map and Status Screens

3.1 Overview

After you log into the Web Configurator, the **Network Map** screen appears. This shows the network connection status of the ZyXEL Device and clients connected to it.

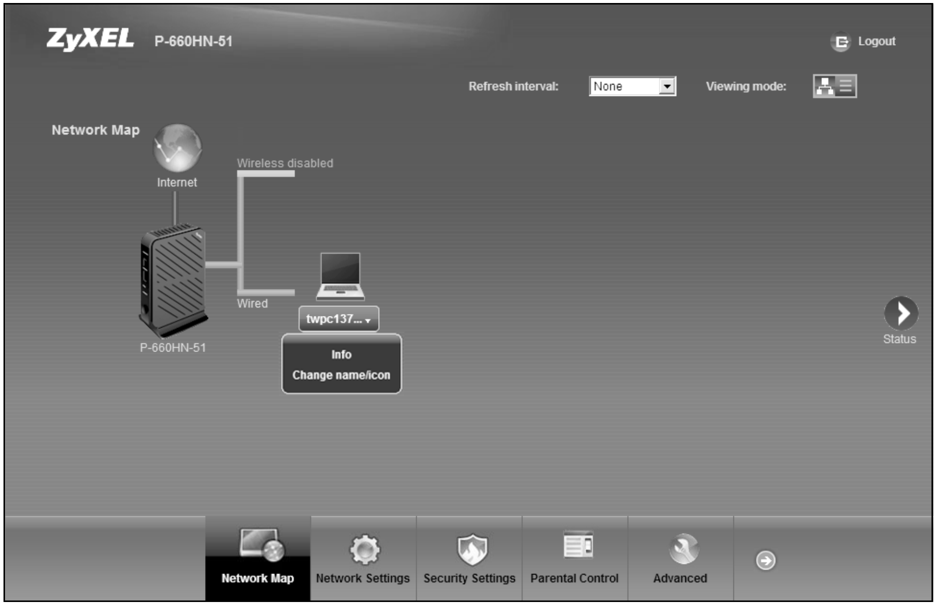
You can use the **Status** screen to look at the current status of the ZyXEL Device, system resources, and interfaces (LAN, WAN, and WLAN).

3.2 The Network Map Screen

Use this screen to view the network connection status of the device and its clients. A warning message appears if there is a connection problem.

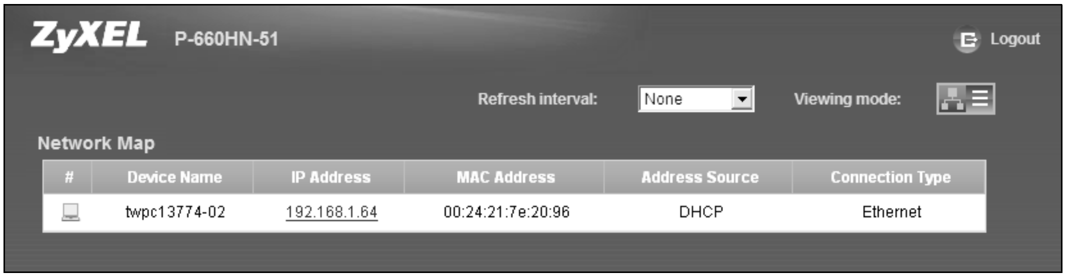
If you prefer to view the status in a list, click **List View** in the **Viewing Mode** selection box. You can configure how often you want the ZyXEL Device to update this screen in **Refresh Interval**.

Figure 8 Network Map: Icon View



Refresh interval: None

Figure 9 Network Map: List View



Refresh interval: None

Network Map

#	Device Name	IP Address	MAC Address	Address Source	Connection Type
💻	twpc13774-02	192.168.1.64	00:24:21:7e:20:96	DHCP	Ethernet

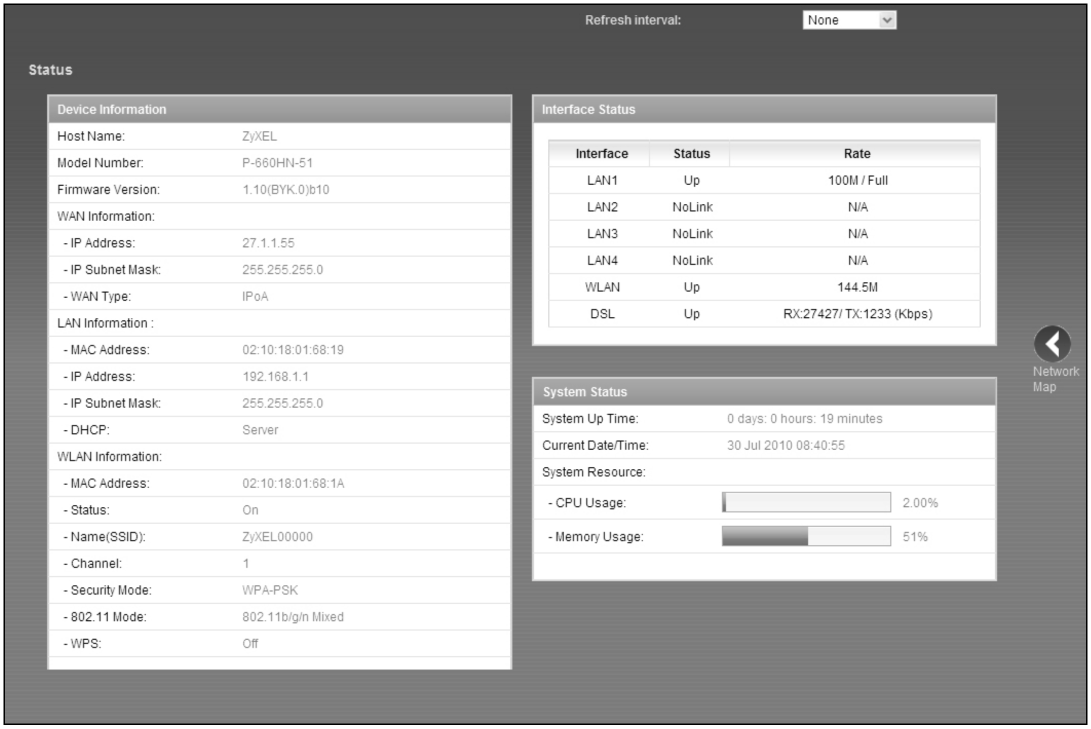
In **Icon View**, if you want to view information about a client, click the client’s name and **Info**. Click the IP address if you want to change it. If you want to change the name or icon of the client, click **Change name/icon**.

In **List View**, you can also view the client’s information and click on the IP address if you want to change it.

3.3 The Status Screen

Use this screen to view the status of the ZyXEL Device. Click **Network Map > Status** to open this screen.

Figure 10 Status Screen



Refresh interval: None

Status

Device Information

Host Name:	ZyXEL
Model Number:	P-660HN-51
Firmware Version:	1.10(BYK.0)b10
WAN Information:	
- IP Address:	27.1.1.55
- IP Subnet Mask:	255.255.255.0
- WAN Type:	IPoA
LAN Information :	
- MAC Address:	02:10:18:01:68:19
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information:	
- MAC Address:	02:10:18:01:68:1A
- Status:	On
- Name(SSID):	ZyXEL00000
- Channel:	1
- Security Mode:	WPA-PSK
- 802.11 Mode:	802.11b/g/n Mixed
- WPS:	Off

Interface Status

Interface	Status	Rate
LAN1	Up	100M / Full
LAN2	NoLink	N/A
LAN3	NoLink	N/A
LAN4	NoLink	N/A
WLAN	Up	144.5M
DSL	Up	RX:27427/ TX:1233 (Kbps)

System Status

System Up Time:	0 days: 0 hours: 19 minutes
Current Date/Time:	30 Jul 2010 08:40:55
System Resource:	
- CPU Usage:	2.00%
- Memory Usage:	51%

Each field is described in the following table.

Table 3 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the ZyXEL Device to update this screen.
Device Information	
Host Name	This field displays the ZyXEL Device system name. It is used for identification.
Model Number	This shows the model number of your ZyXEL Device.
Firmware Version	This is the current version of the firmware inside the device.
WAN Information	
MAC Address	This shows the WAN Ethernet adapter MAC (Media Access Control) Address of your device. This field is available only when your WAN type is **IPoE** or **PPPoE**.
IP Address	This field displays the current IP address of the ZyXEL Device in the WAN.

Table 3 Status Screen (continued)

LABEL	DESCRIPTION
IP Subnet Mask	This field displays the current subnet mask in the WAN. This field is available only when your WAN type is **IPoE** or **IPoA**.
WAN Type	This field displays the current the WAN type.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC (Media Access Control) Address of your device.
IP Address	This is the current IP address of the ZyXEL Device in the LAN.
IP Subnet Mask	This is the current subnet mask in the LAN.
DHCP	This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are: **Server** - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The ZyXEL Device is not providing any DHCP services to the LAN.
WLAN Information	
MAC Address	This shows the wireless adapter MAC (Media Access Control) Address of your device.
Status	This displays whether WLAN is activated.
Name (SSID)	This is the descriptive name used to identify the ZyXEL Device in a wireless LAN.
Channel	This is the channel number used by the ZyXEL Device now.
Security Mode	This displays the type of security mode the ZyXEL Device is using in the wireless LAN.
802.11 Mode	This displays the type of 802.11 mode the ZyXEL Device is using in the wireless LAN.
WPS	This displays whether WPS is activated.
Interface Status	
Interface	This column displays each interface the ZyXEL Device has.

Table 3 Status Screen (continued)

LABEL	DESCRIPTION
Status	This field indicates whether or not the ZyXEL Device is using the interface. For the DSL interface, this field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation. For the LAN interface, this field displays **Up** when the ZyXEL Device is using the interface and **Down** when the ZyXEL Device is not using the interface. For the WLAN interface, it displays **Active** when WLAN is enabled or **InActive** when WLAN is disabled.
Rate	For the LAN interface, this displays the port speed and duplex setting. For the DSL interface, it displays the downstream and upstream transmission rate. For the WLAN interface, it displays the maximum transmission rate when WLAN is enabled or **N/A** when WLAN is disabled.
System Status	
System Up Time	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it.
Current Date/Time	This field displays the current date and time in the ZyXEL Device. You can change this in **Advanced > Time Setting**.
System Resource	
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using QoS; see Chapter 17 on page 211).
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the ZyXEL Device is probably becoming unstable, and you should restart the device. See Section 28.2 on page 267, or turn off the device (unplug the power) for a few seconds.

4

Tutorials

4.1 Overview

This chapter shows you how to use the ZyXEL Device's various features.

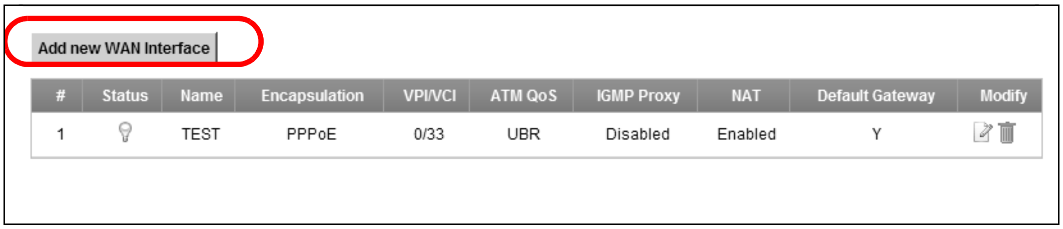
- Setting Up Your DSL Connection Using PPPoE, see page 41
- Setting Up a Secure Wireless Network, see page 44
- Setting Up Multiple Wireless Groups, see page 52
- Configuring Static Route for Routing to Another Network, see page 55
- Access the ZyXEL Device Using DDNS, see page 58

4.2 Setting Up Your DSL Connection Using PPPoE

This tutorial shows you how to set up your Internet connection using the Web Configurator.

If you connect to the Internet through a DSL connection, use the information from your Internet Service Provider (ISP) to configure the ZyXEL Device. Be sure to contact your service provider for any information you need to configure the **Broadband** screens.

1 Click **Network Settings > Broadband** to open the following screen. Click **Add new WAN Interface**.



#	Status	Name	Encapsulation	VPI/VCI	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1	💡	TEST	PPPoE	0/33	UBR	Disabled	Enabled	Y	✎ 🗑

2 In this example, the DSL connection has the following information.

General	
Connection Name	MyDSLConnection
Connection Mode	Routing
Encapsulation	PPPoE
ATM PVC Configuration	
VPI/VCI	36/48
Encapsulation Mode	LLC/SNAP-Bridging
Service Category	UBR without PCR
Account Information	
PPP User Name	1234@DSL-Ex.com
PPP Password	ABCDEF!
PPPoE Service Name	My DSL
Static IP Address	192.168.1.32
Others	PPPoE Passthrough: Disabled NAT: Enabled IGMP Multicast Proxy: Enabled Apply as Default Gateway: Enable Static DNS: Server 1: 192.168.1.254 Server 2: 192.168.1.253

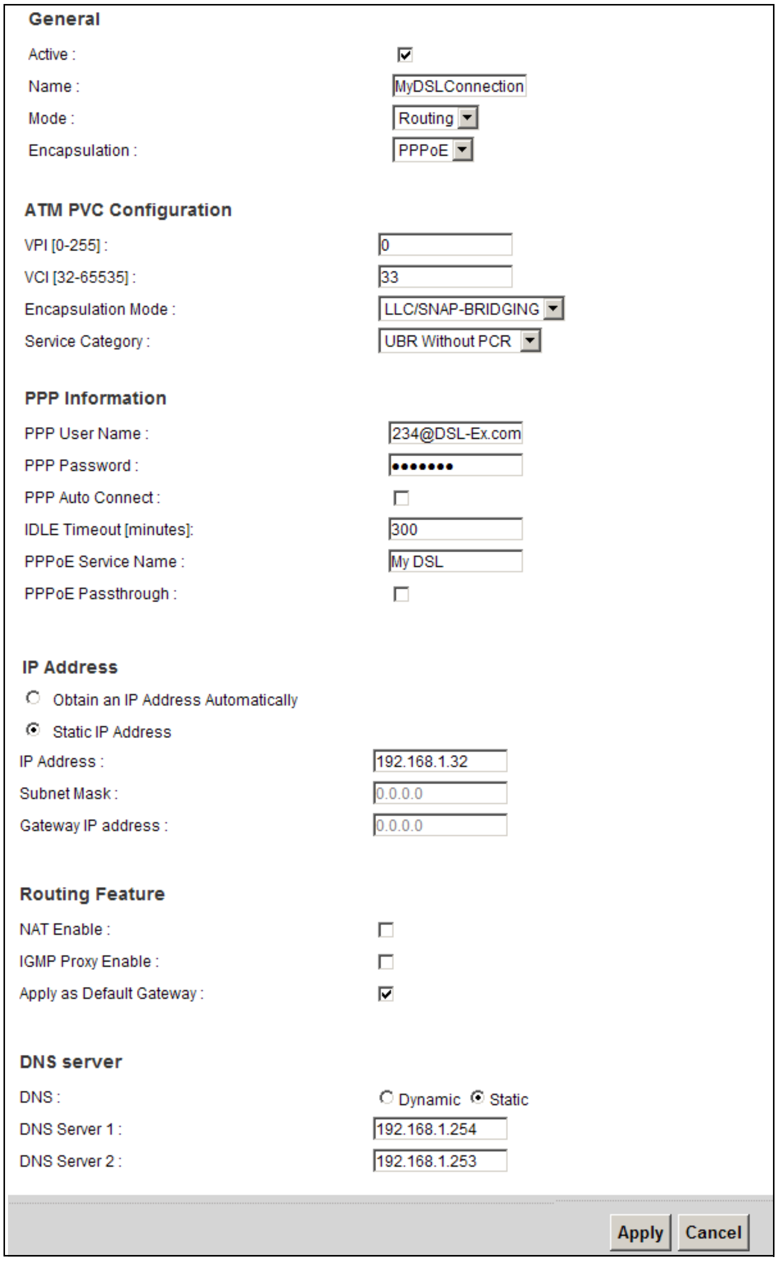
3 Select the **Active** check box. Enter the **General** and **ATM PVC Configuration** settings as provided above.

Choose the **Encapsulation** specified by your DSL service provider. For this example, the service provider requires a username and password to establish Internet connection. Therefore, select **PPPoE** as the WAN encapsulation type.

4 Enter the account information provided to you by your DSL service provider.

5 Configure this rule as your default Internet connection by selecting the **Apply as Default Gateway** check box. Then select DNS as **Static** and enter the DNS server addresses provided to you, such as **192.168.1.254** (DNS server1)/ **192.168.1.253** (DNS server2).

6 Click **Apply** to save your settings.



General

Active : ☑

Name : MyDSLConnection

Mode : Routing

Encapsulation : PPPoE

ATM PVC Configuration

VPI [0-255] : 0

VCI [32-65535] : 33

Encapsulation Mode : LLC/SNAP-BRIDGING

Service Category : UBR Without PCR

PPP Information

PPP User Name : 234@DSL-Ex.com

PPP Password : •••••••

PPP Auto Connect : □

IDLE Timeout [minutes]: 300

PPPoE Service Name : My DSL

PPPoE Passthrough : □

IP Address

○ Obtain an IP Address Automatically

● Static IP Address

IP Address : 192.168.1.32

Subnet Mask : 0.0.0.0

Gateway IP address : 0.0.0.0

Routing Feature

NAT Enable : □

IGMP Proxy Enable : □

Apply as Default Gateway : ☑

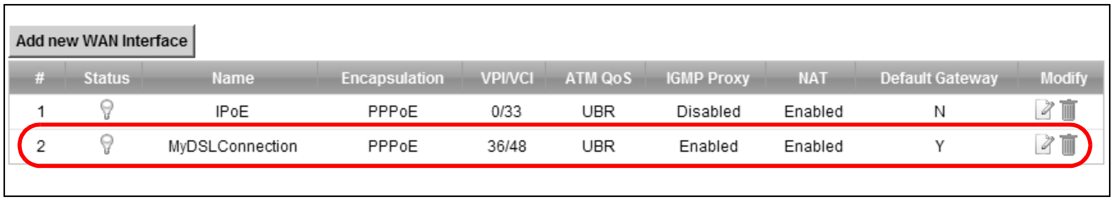
DNS server

DNS : ○ Dynamic ● Static

DNS Server 1 : 192.168.1.254

DNS Server 2 : 192.168.1.253

7 You should see a summary of your new DSL connection setup in the **Broadband** screen as follows.

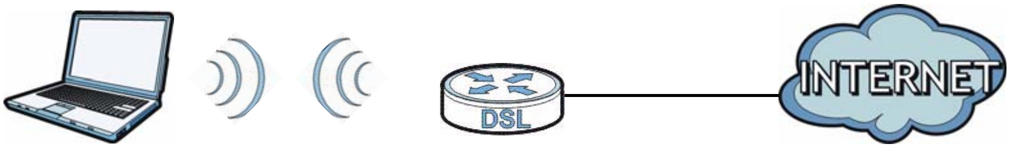


#	Status	Name	Encapsulation	VPI/VCI	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1		IPoE	PPPoE	0/33	UBR	Disabled	Enabled	N	
2		MyDSLConnection	PPPoE	36/48	UBR	Enabled	Enabled	Y	

Try to connect to a website, such as zyxel.com to see if you have correctly set up your Internet connection. Be sure to contact your service provider for any information you need to configure the WAN screens.

4.3 Setting Up a Secure Wireless Network

This tutorial is an example of setting up a wireless network to have wireless Internet access. In this wireless network, the ZyXEL Device serves as an access point (AP), and the notebook is the wireless client. The wireless client can access the Internet through the AP.



You have to configure the wireless network settings on the ZyXEL Device. You can set up a wireless network using WPS (Section 4.3.2 on page 46) or manual configuration (Section 4.3.3 on page 51).

4.3.1 Configuring the Wireless Network Settings

This example uses the following parameters to set up a wireless network.

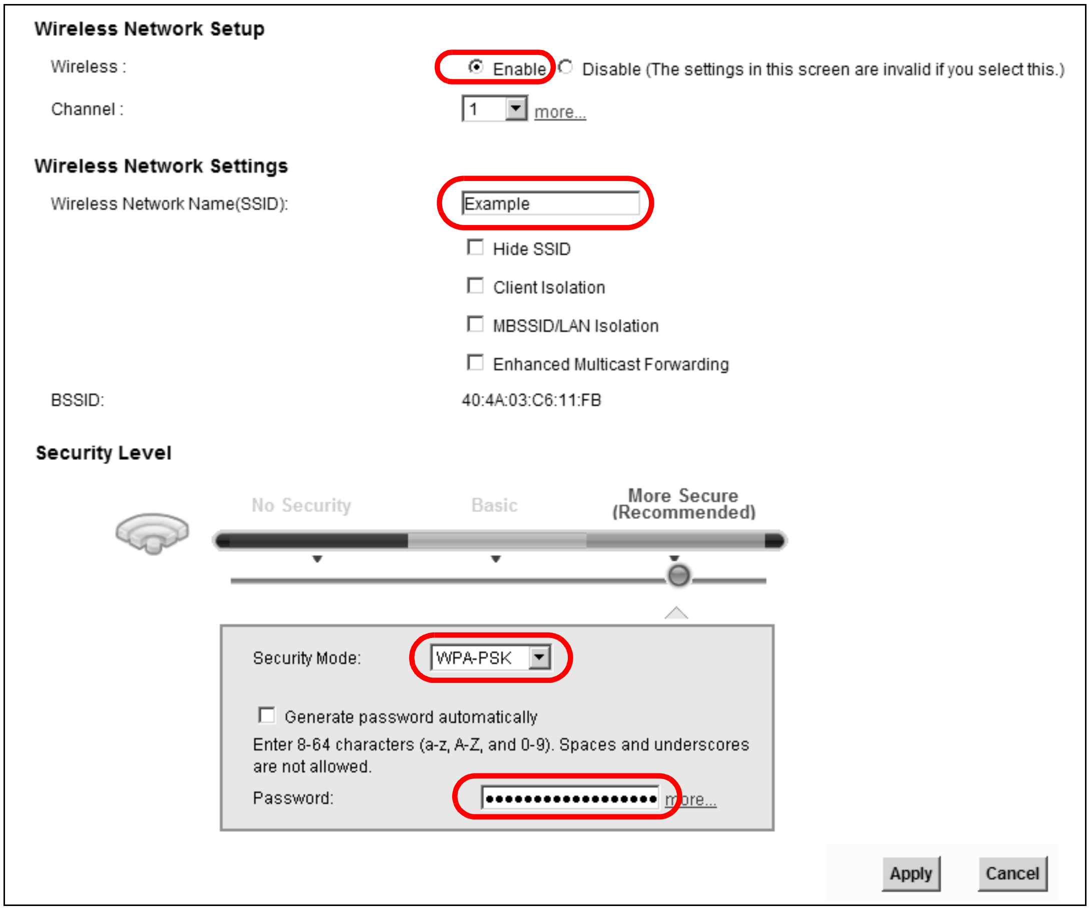
SSID	Example
Security Mode	WPA-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	802.11b/g/n Mixed

1 Click **Network Settings** > **Wireless** to open the **General** screen.

2 Select Enable to activate the wireless network.

3 Enter the SSID name in **Wireless Network Name**.

4 Select **More Secure** as the security level and **WPA-PSK** as the security mode. Configure the screen using the provided parameters (see page 44). Click **Apply**.



Wireless Network Setup

Wireless : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Channel : 1 more...

Wireless Network Settings

Wireless Network Name(SSID): Example

□ Hide SSID

□ Client Isolation

□ MBSSID/LAN Isolation

□ Enhanced Multicast Forwarding

BSSID: 40:4A:03:C6:11:FB

Security Level

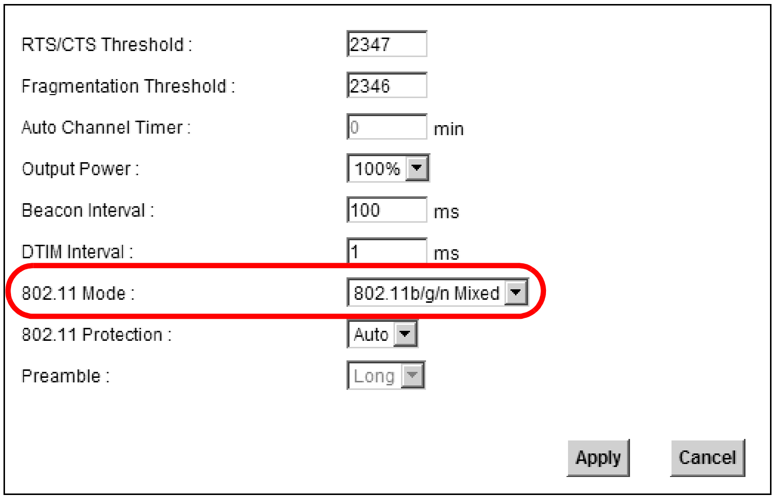
Security Mode: WPA-PSK

□ Generate password automatically

Enter 8-64 characters (a-z, A-Z, and 0-9). Spaces and underscores are not allowed.

Password: •••••••••••••••••• more...

5 Go to the **Wireless > Others** screen and select **802.11b/g/n Mixed** in the **802.11 Mode** field. Click **Apply**.



RTS/CTS Threshold : 2347

Fragmentation Threshold : 2346

Auto Channel Timer : 0 min

Output Power : 100%

Beacon Interval : 100 ms

DTIM Interval : 1 ms

802.11 Mode : 802.11b/g/n Mixed

802.11 Protection : Auto

Preamble : Long

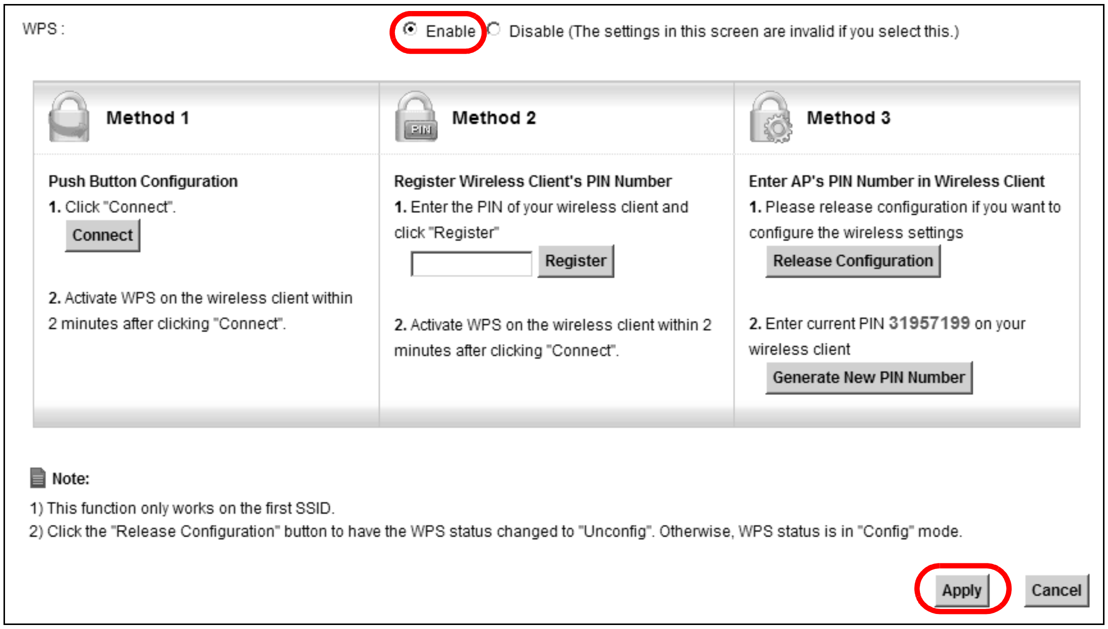
You can now use the WPS feature to establish a wireless connection between your notebook and the ZyXEL Device (see Section 4.3.2 on page 46). You can also use the notebook's wireless client to search for the ZyXEL Device (see Section 4.3.3 on page 51).

4.3.2 Using WPS

This section shows you how to set up a wireless network using WPS. It uses the ZyXEL Device as the AP and ZyXEL NWD210N as the wireless client which connects to the notebook.

f your wireless devices display the WPS logo, you can use Wi-Fi Protected Setup (WPS) to add wireless devices to your wireless network.

The ZyXEL Device's WPS function must be enabled before using WPS. Log into ZyXEL Device's web configurator and go to the **Network Settings > Wireless > WPS** screen. Enable the WPS function and click **Apply**.



WPS : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Method 1

Push Button Configuration

1. Click "Connect".

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 2

Register Wireless Client's PIN Number

1. Enter the PIN of your wireless client and click "Register"

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 3

Enter AP's PIN Number in Wireless Client

1. Please release configuration if you want to configure the wireless settings

2. Enter current PIN **31957199** on your wireless client

Note:

1) This function only works on the first SSID.

2) Click the "Release Configuration" button to have the WPS status changed to "Unconfig". Otherwise, WPS status is in "Config" mode.

There are three WPS methods to set up the wireless client settings:

- **Method 1- Push Button Configuration (PBC)** - simply press a button. This is the easier of the two methods.
- **Method 2- Register Wireless Client's PIN Number** - Both the ZyXEL Device and the wireless client has a Personal Identification Number (PIN). Enter the wireless client's PIN number and register it on the ZyXEL Device to download the wireless network settings from the ZyXEL Device.
- **Method 3- Enter AP's PIN Number in Wireless Client -** Configure a PIN number on the ZyXEL Device. Enter the ZyXEL Device's PIN number and register it on the wireless client.

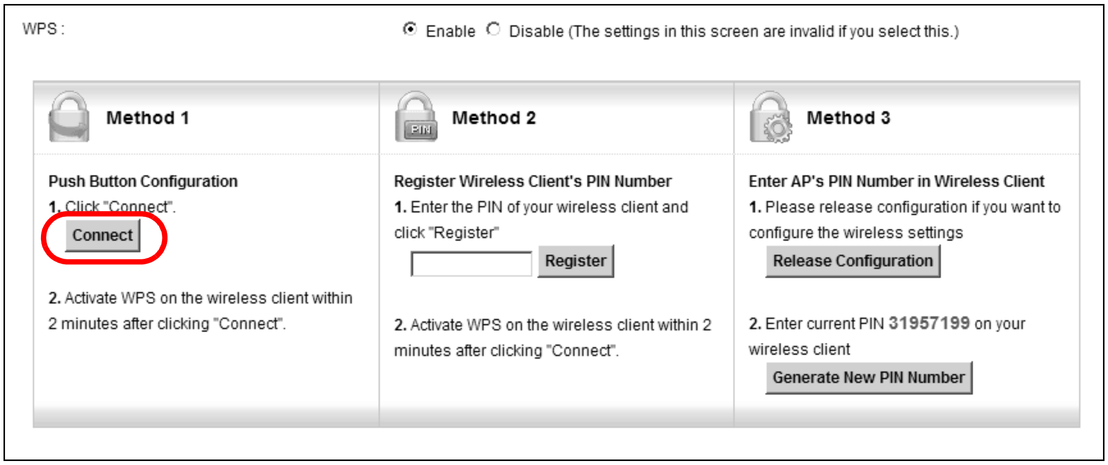
Method 1: Push Button Configuration (PBC)

1 Make sure that your ZyXEL Device is turned on and your notebook is within the cover range of the wireless signal.

2 Make sure that you have installed the wireless client driver and utility in your notebook.

3 In the wireless client utility, go to the WPS setting page. Enable WPS and press the WPS button (**Start** or **WPS** button).

4 Push and hold the **WPS** button located on the ZyXEL Device's front panel for 5 to 10 seconds. The WLAN/WPS LED starts blinking orange. Alternatively, you can log into ZyXEL Device's web configurator and go to the **Network Settings > Wireless > WPS** screen. Click the **Connect** button.



WPS : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Method 1

Push Button Configuration

1. Click "Connect".

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 2

Register Wireless Client's PIN Number

1. Enter the PIN of your wireless client and click "Register"

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 3

Enter AP's PIN Number in Wireless Client

1. Please release configuration if you want to configure the wireless settings

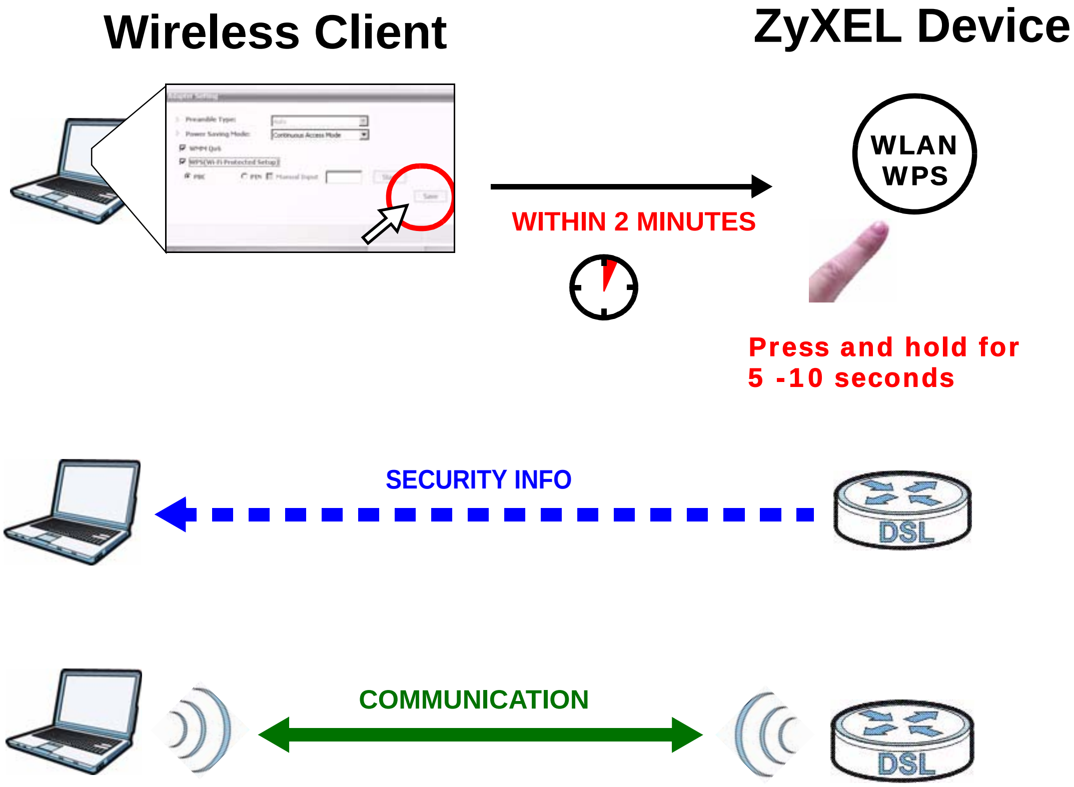
2. Enter current PIN 31957199 on your wireless client

Note: Your ZyXEL Device has a **WLAN/WPS** button located on its front panel as well as a **Connect** button in its configuration utility. Both buttons have exactly the same function: you can use one or the other.

Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The ZyXEL Device sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the ZyXEL Device securely.

The following figure shows you an example of how to set up a wireless network and its security by pressing a button on both ZyXEL Device and wireless client.

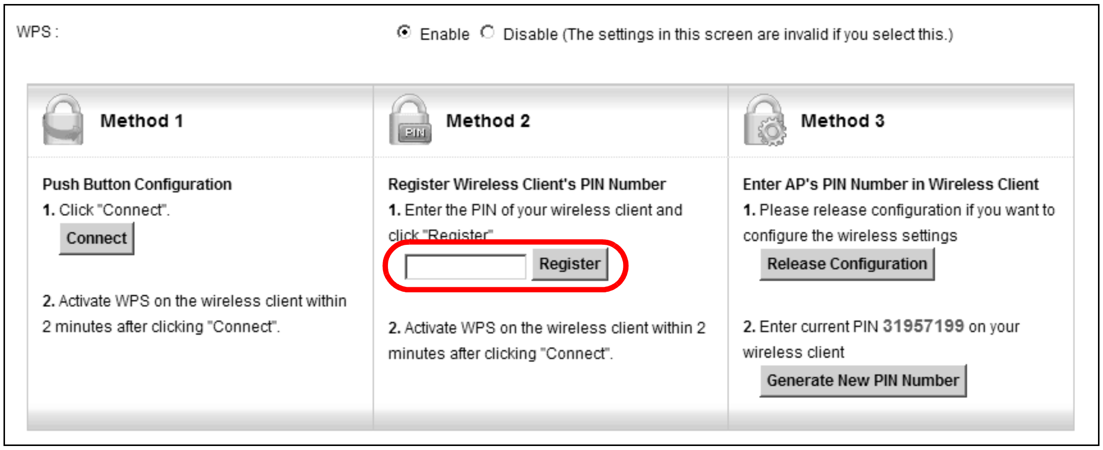


Method 2: Register Wireless Client’s PIN Number

When you use the PIN configuration method, you need to use both the ZyXEL Device’s web configurator and the wireless client’s utility.

1 Launch your wireless client’s configuration utility. Go to the WPS settings and select the PIN method to get the wireless client’s PIN number.

2 Log into the web configurator and go to the **Network Settings > Wireless > WPS** screen. Enter the PIN number of the wireless client and click the **Register** button. Activate WPS function on the wireless client utility screen within two minutes.



WPS : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Method 1

Push Button Configuration

1. Click "Connect".

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 2

Register Wireless Client's PIN Number

1. Enter the PIN of your wireless client and click "Register".

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 3

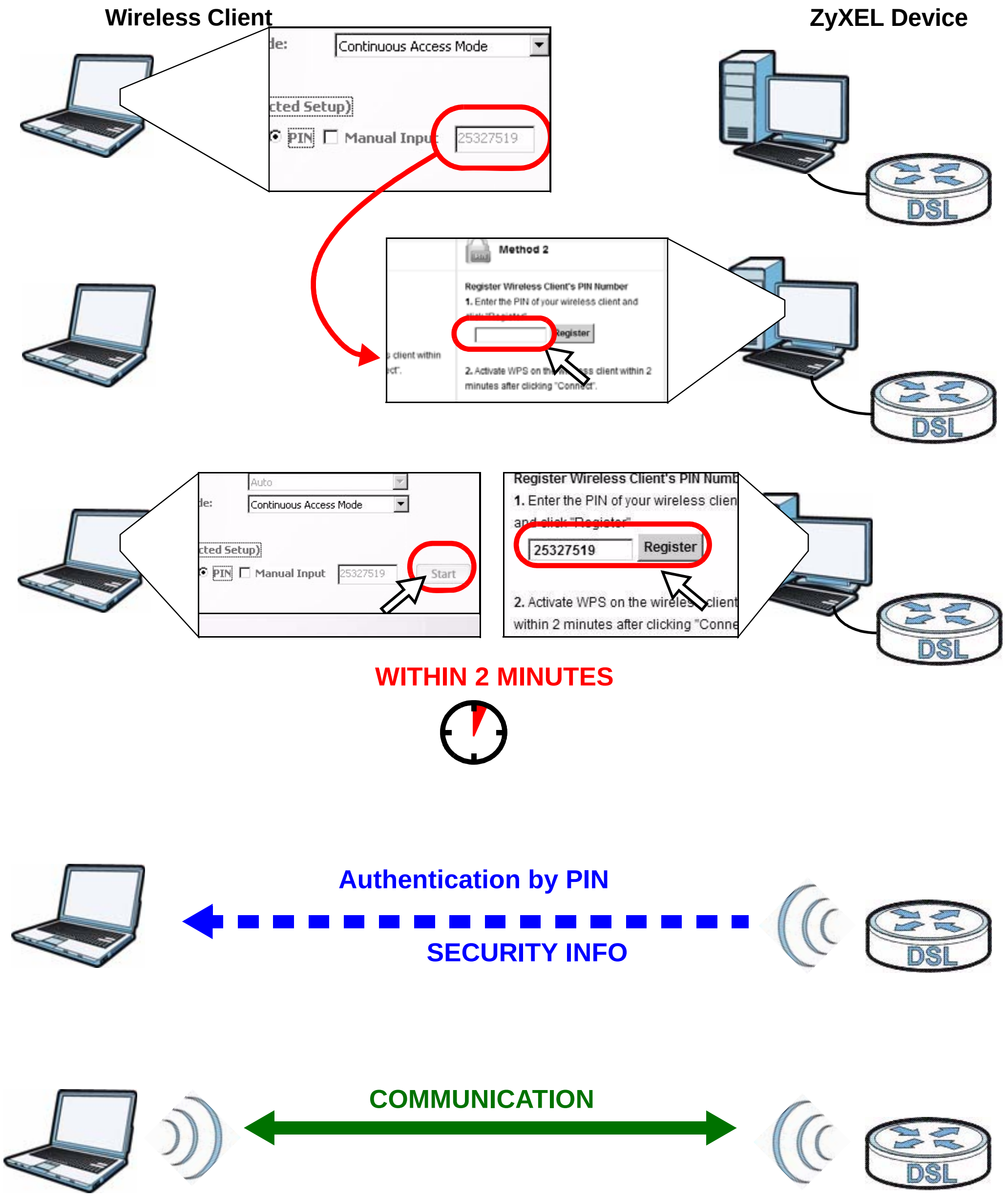
Enter AP's PIN Number in Wireless Client

1. Please release configuration if you want to configure the wireless settings

2. Enter current PIN 31957199 on your wireless client

3 The ZyXEL Device authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. The wireless client is then able to communicate with the ZyXEL Device securely.

The following figure shows you how to set up a wireless network and its security on a ZyXEL Device and a wireless client by using PIN method.


Wireless Client
ZyXEL Device
de:
Continuous Access Mode
cted Setup)
PIN
Manual Input
25327519
Method 2
Register Wireless Client's PIN Number
1. Enter the PIN of your wireless client and click "Register".
Register
client within
ct".
2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".
Auto
de:
Continuous Access Mode
cted Setup)
PIN
Manual Input
25327519
Start
Register Wireless Client's PIN Numb
1. Enter the PIN of your wireless clien
and click "Register".
25327519
Register
2. Activate WPS on the wireless client
within 2 minutes after clicking "Conne
WITHIN 2 MINUTES
DSL
Authentication by PIN
SECURITY INFO
COMMUNICATION

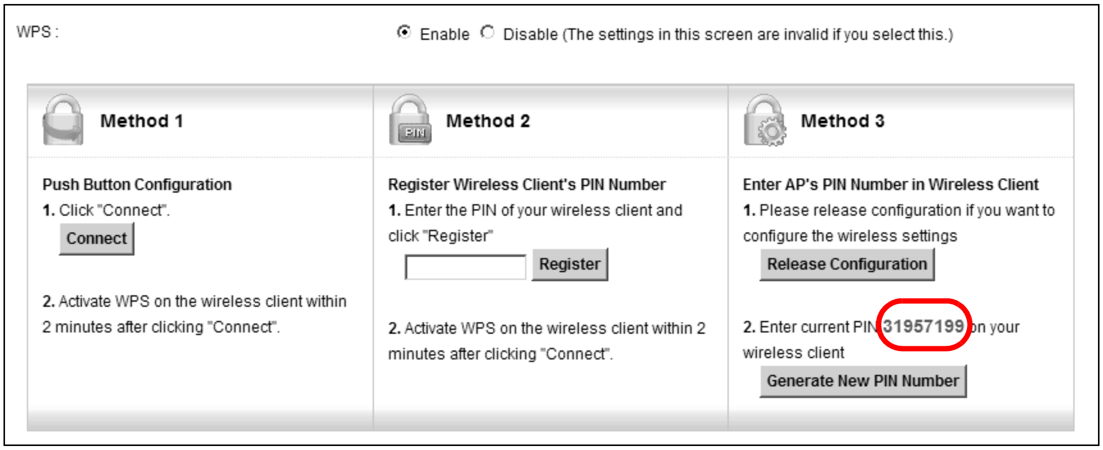
Method 3- Enter AP’s PIN Number in Wireless Client

1 Log into the web configurator and go to the **Network Settings > Wireless > WPS** screen.

2 Click the **Release Configuration** button to release all wireless settings on the ZyXEL Device.

3 Copy the PIN number of the ZyXEL Device shown in step 2 of Method 3 . You can click on the **Generate New PIN Number** button if you want the ZyXEL Device to auto-generate a new PIN number.

4 Enter the PIN number and register it on the wireless client’s WPS setting. Activate WPS function on the wireless client utility screen within two minutes.



WPS : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Method 1

Push Button Configuration

1. Click "Connect".

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 2

Register Wireless Client's PIN Number

1. Enter the PIN of your wireless client and click "Register"

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 3

Enter AP's PIN Number in Wireless Client

1. Please release configuration if you want to configure the wireless settings

2. Enter current PIN 31957199 on your wireless client

5 The wireless client authenticates the ZyXEL Device and sends the proper configuration settings to the ZyXEL Device. This may take up to two minutes. The ZyXEL Device is then able to communicate with the wireless client securely.

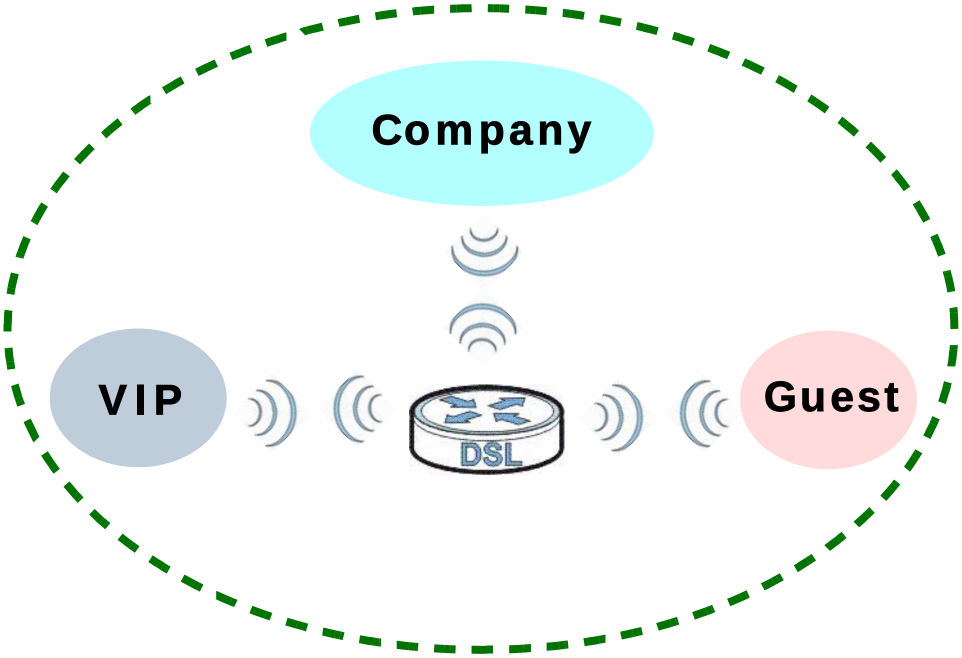
4.3.3 Without WPS

Use the wireless adapter’s utility installed on the notebook to search for the “Example” SSID. Then enter the “DoNotStealMyWirelessNetwork” pre-shared key to establish an wireless Internet connection.

Note: The ZyXEL Device supports IEEE 802.11b and IEEE 802.11g wireless clients. Make sure that your notebook or computer’s wireless adapter supports one of these standards.

4.4 Setting Up Multiple Wireless Groups

You want to create different wireless network groups for different types of users in your company as shown in the following figure. Each group has its own SSID and security mode.

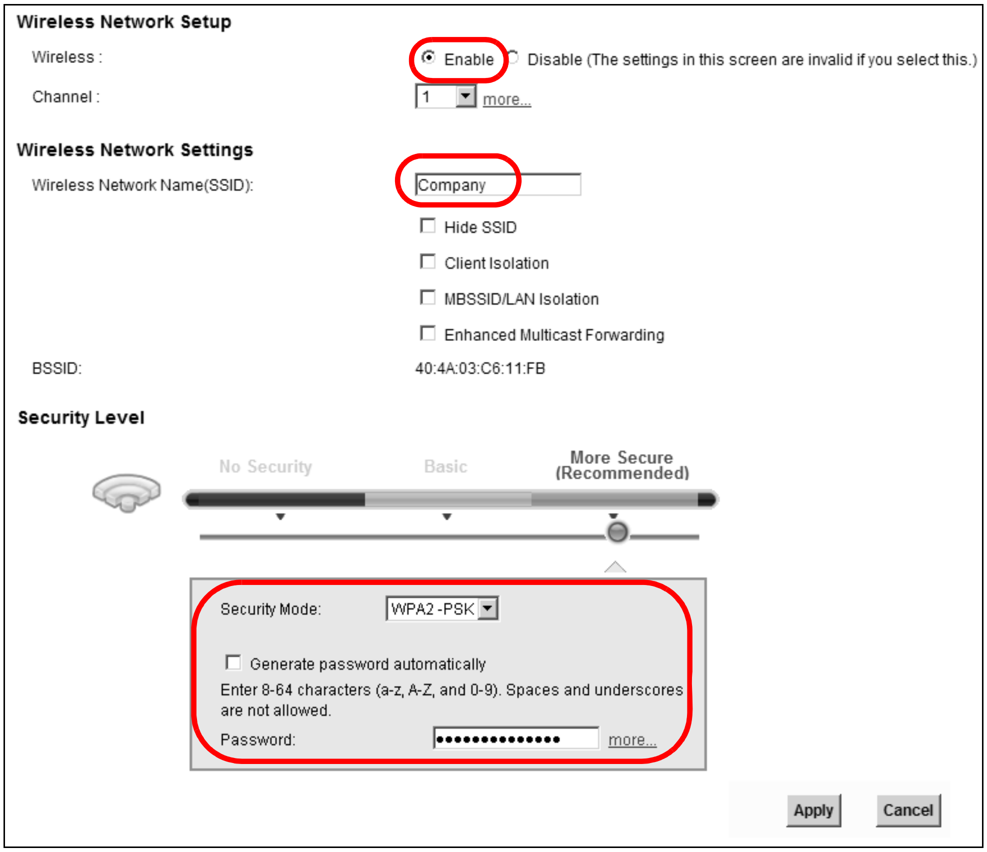


- Employees in the company will use a general **Company** wireless network group.
- Higher management level and important visitors will use the **VIP** group.
- Visiting guests will use the **Guest** group, which has a lower security mode.

Follow the parameters below to set up the wireless network groups.

	COMPANY	VIP	GUEST
SSID	Company	VIP	Guest
Security Level	More Secure	More Secure	Basic
Security Mode	WPA2-PSK	WPA2-PSK	Static WEP
Pre-Shared Key	ForCompanyOnly	ForVIPOnly	Guest

1 Click **Network Settings > Wireless** to open the **General** screen. Use this screen to set up the company's general wireless network group. Configure the screen using the provided parameters and click **Apply**.



Wireless Network Setup

Wireless : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Channel : 1 more...

Wireless Network Settings

Wireless Network Name(SSID): Company

□ Hide SSID

□ Client Isolation

□ MBSSID/LAN Isolation

□ Enhanced Multicast Forwarding

BSSID: 40:4A:03:C6:11:FB

Security Level

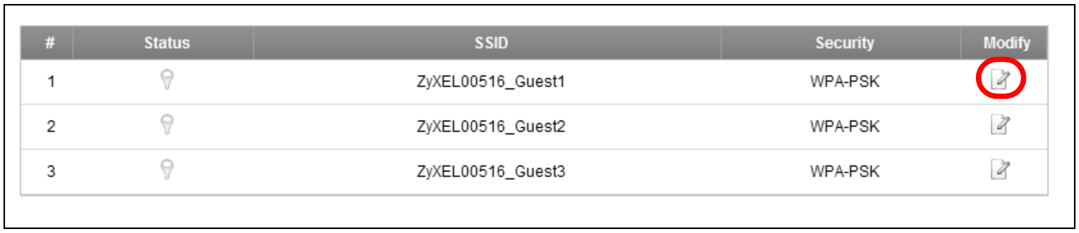
Security Mode: WPA2 -PSK

□ Generate password automatically

Enter 8-64 characters (a-z, A-Z, and 0-9). Spaces and underscores are not allowed.

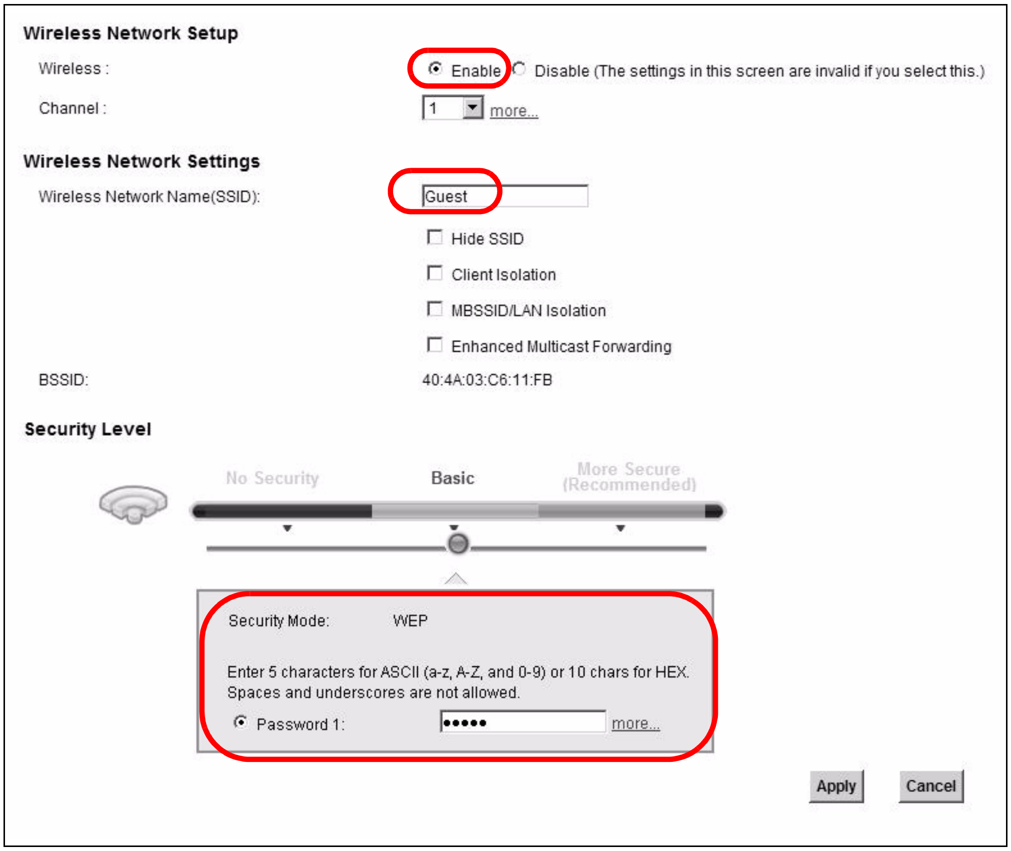
Password: ●●●●●●●●●●●●●● more...

2 Click **Network Settings > Wireless > More AP** to open the following screen. Click the **Edit** icon to configure the second wireless network group.



#	Status	SSID	Security	Modify
1		ZyXEL00516_Guest1	WPA-PSK	
2		ZyXEL00516_Guest2	WPA-PSK	
3		ZyXEL00516_Guest3	WPA-PSK	

3 Configure the screen using the provided parameters and click **Apply**.



Wireless Network Setup

Wireless : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Channel : 1 more...

Wireless Network Settings

Wireless Network Name(SSID): Guest

□ Hide SSID

□ Client Isolation

□ MBSSID/LAN Isolation

□ Enhanced Multicast Forwarding

BSSID: 40:4A:03:C6:11:FB

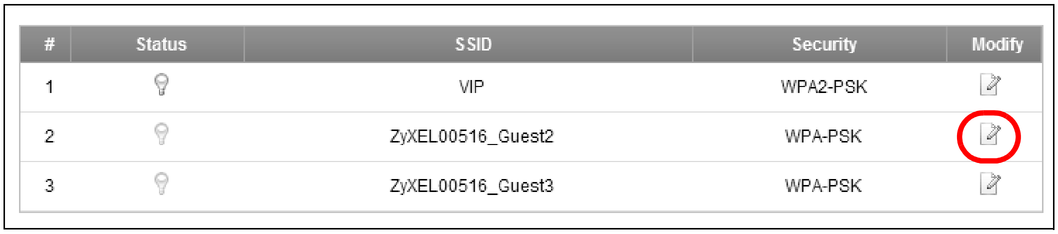
Security Level

Security Mode: WEP

Enter 5 characters for ASCII (a-z, A-Z, and 0-9) or 10 chars for HEX. Spaces and underscores are not allowed.

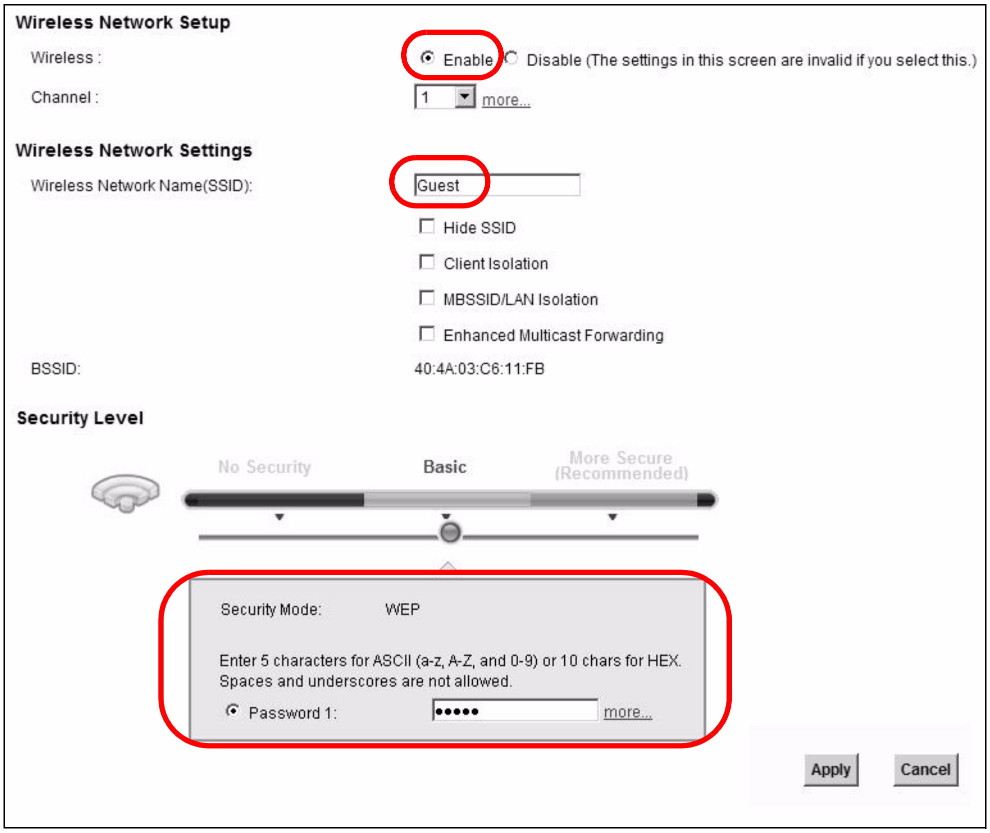
● Password 1: ••••• more...

4 In the **More AP** screen, click the **Edit** icon to configure the third wireless network group.



#	Status	SSID	Security	Modify
1	💡	VIP	WPA2-PSK	✎
2	💡	ZyXEL00516_Guest2	WPA-PSK	✎
3	💡	ZyXEL00516_Guest3	WPA-PSK	✎

5 Configure the screen using the provided parameters and click **Apply**.



Wireless Network Setup

Wireless : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Channel : 1 more...

Wireless Network Settings

Wireless Network Name(SSID): Guest

□ Hide SSID

□ Client Isolation

□ MBSSID/LAN Isolation

□ Enhanced Multicast Forwarding

BSSID: 40:4A:03:C6:11:FB

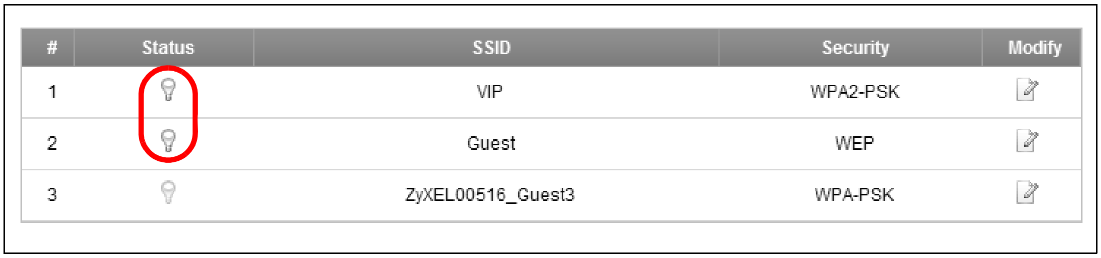
Security Level

Security Mode: WEP

Enter 5 characters for ASCII (a-z, A-Z, and 0-9) or 10 chars for HEX. Spaces and underscores are not allowed.

● Password 1: ●●●●● more...

6 Check the status of **VIP** and **Guest** in the **More AP** screen. The yellow bulbs signify that the SSIDs are active and ready for wireless access.

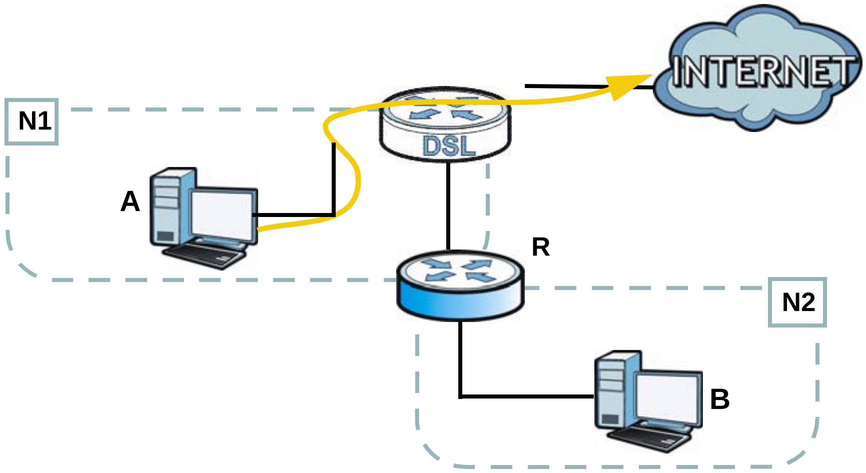


#	Status	SSID	Security	Modify
1	💡	VIP	WPA2-PSK	✎
2	💡	Guest	WEP	✎
3	💡	ZyXEL00516_Guest3	WPA-PSK	✎

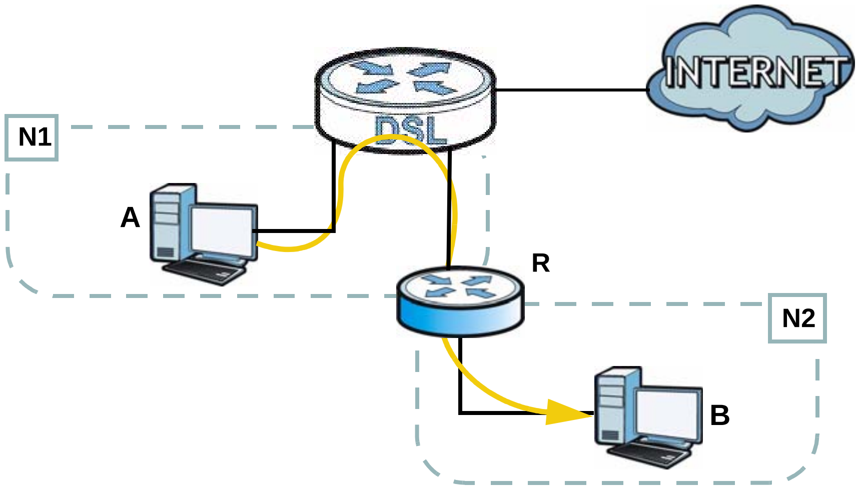
4.5 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the ZyXEL Device’s LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the ZyXEL Device’s LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the ZyXEL Device’s WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the ZyXEL Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the ZyXEL Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.



This tutorial uses the following example IP settings:

Table 4 IP Settings in this Tutorial

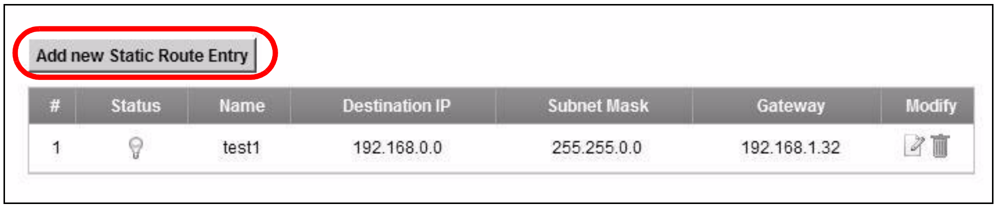
DEVICE / COMPUTER	IP ADDRESS
The ZyXEL Device's WAN	172.16.1.1
The ZyXEL Device's LAN	192.168.1.1
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

To configure a static route to route traffic from **N1** to **N2**:

1 Log into the ZyXEL Device's Web Configurator in advanced mode.

2 Click **Advanced** > **Routing**.

3 Click **Add New Static Route Entry** in the **Static Route** screen.



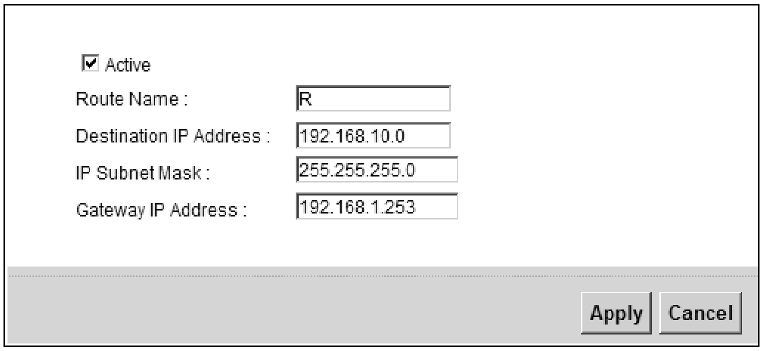
#	Status	Name	Destination IP	Subnet Mask	Gateway	Modify
1		test1	192.168.0.0	255.255.0.0	192.168.1.32	

4 Configure the **Static Route Setup** screen using the following settings:

4a Select the **Active** check box. Enter the **Route Name** as **R**.

4b Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.

4c Type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.



☑ Active

Route Name : R

Destination IP Address : 192.168.10.0

IP Subnet Mask : 255.255.255.0

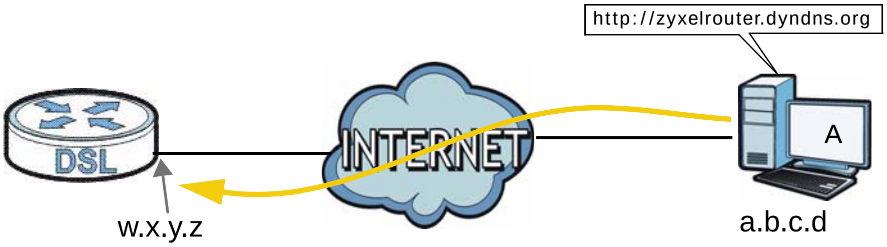
Gateway IP Address : 192.168.1.253

4a Click **Apply**.

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.

4.6 Access the ZyXEL Device Using DDNS

If you connect your ZyXEL Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The ZyXEL Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the ZyXEL Device using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial shows you how to:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your ZyXEL Device
- Testing the DDNS Setting

Note: If you have a private WAN IP address, then you cannot use DDNS.

4.6.1 Registering a DDNS Account on www.dyndns.org

1 Open a browser and type **http://www.dyndns.org**.

2 Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.

3 Log into www.dyndns.org using your account.

4 Add a new DDNS host name. This tutorial uses the following settings as an example.

- Hostname: **zyxelrouter.dyndns.org**
- Service Type: **Host with IP address**

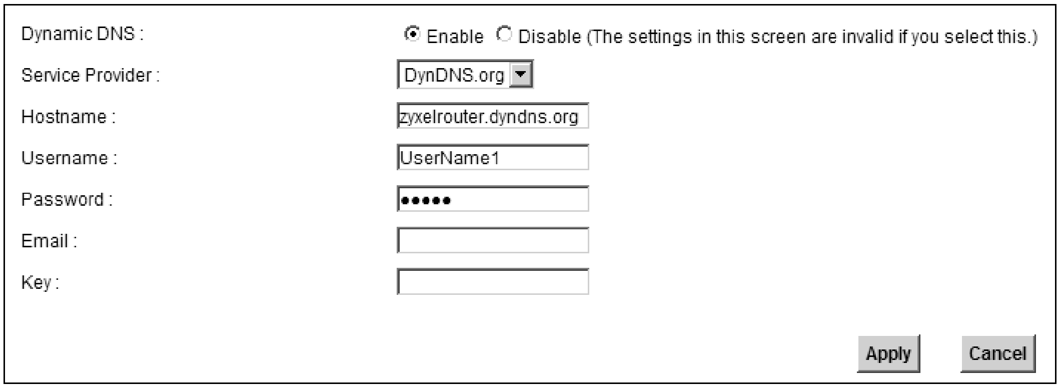
- IP Address: Enter the WAN IP address that your ZyXEL Device is currently using. You can find the IP address on the ZyXEL Device’s Web Configurator **Status** page.

Then you will need to configure the same account and host name on the ZyXEL Device later.

4.6.2 Configuring DDNS on Your ZyXEL Device

Configure the following settings in the **Advanced > DNS Setting > Dynamic DNS** screen.

- Select **Enable Dynamic DNS**.
- Select **DynDNS.org** as the service provider.
- Type **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**).



Dynamic DNS :	● Enable ○ Disable (The settings in this screen are invalid if you select this.)
Service Provider :	DynDNS.org
Hostname :	zyxelrouter.dyndns.org
Username :	UserName1
Password :	●●●●●
Email :	
Key :	

Click **Apply**.

4.6.3 Testing the DDNS Setting

Now you should be able to access the ZyXEL Device from the Internet. To test this:

1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

2 Type **http://zyxelrouter.dyndns.org** and press [Enter].

3 The ZyXEL Device’s login page should appear. You can then log into the ZyXEL Device and manage it.

PART II

Technical Reference

5

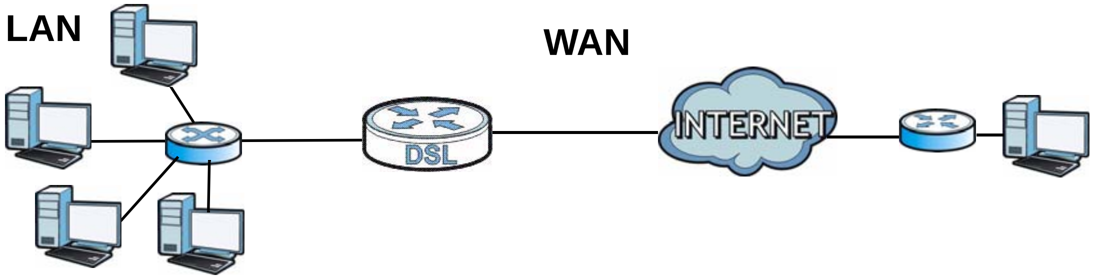
Broadband

5.1 Overview

This chapter describes how to configure WAN settings from the **Broadband** screen. Use this screen to configure your ZyXEL Device for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks (such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 11 LAN and WAN



5.1.1 What You Need to Know

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPPoA, they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the ZyXEL Device, which makes it accessible from an outside network. It is used by the ZyXEL Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the ZyXEL Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet encapsulation method).

Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just one.

IGMP

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 and 3 are improvements over version 1, but IGMP version 1 is still in wide use.

Finding Out More

See Section 5.3 on page 73 for technical background information on WAN.

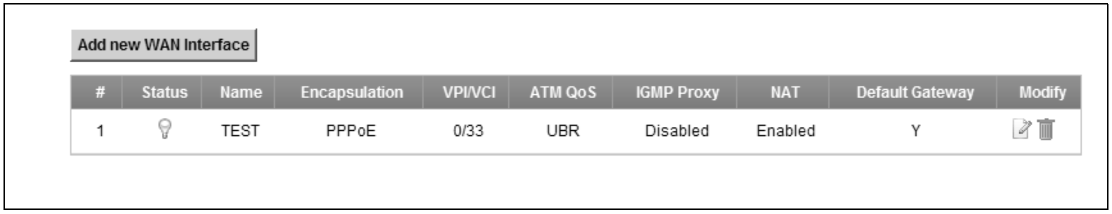
5.1.2 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

5.2 The Broadband Screen

Use this screen to change your ZyXEL Device’s Internet access settings. Click **Network Settings> Broadband** from the menu. The summary table shows you the configured WAN services (connections) on the ZyXEL Device.

Figure 12 Network Settings > Broadband



Add new WAN Interface

#	Status	Name	Encapsulation	VPI/VCI	ATM QoS	IGMP Proxy	NAT	Default Gateway	Modify
1	●	TEST	PPPoE	0/33	UBR	Disabled	Enabled	Y	✎ 🗑

The following table describes the labels in this screen.

Table 5 Network Settings > Broadband

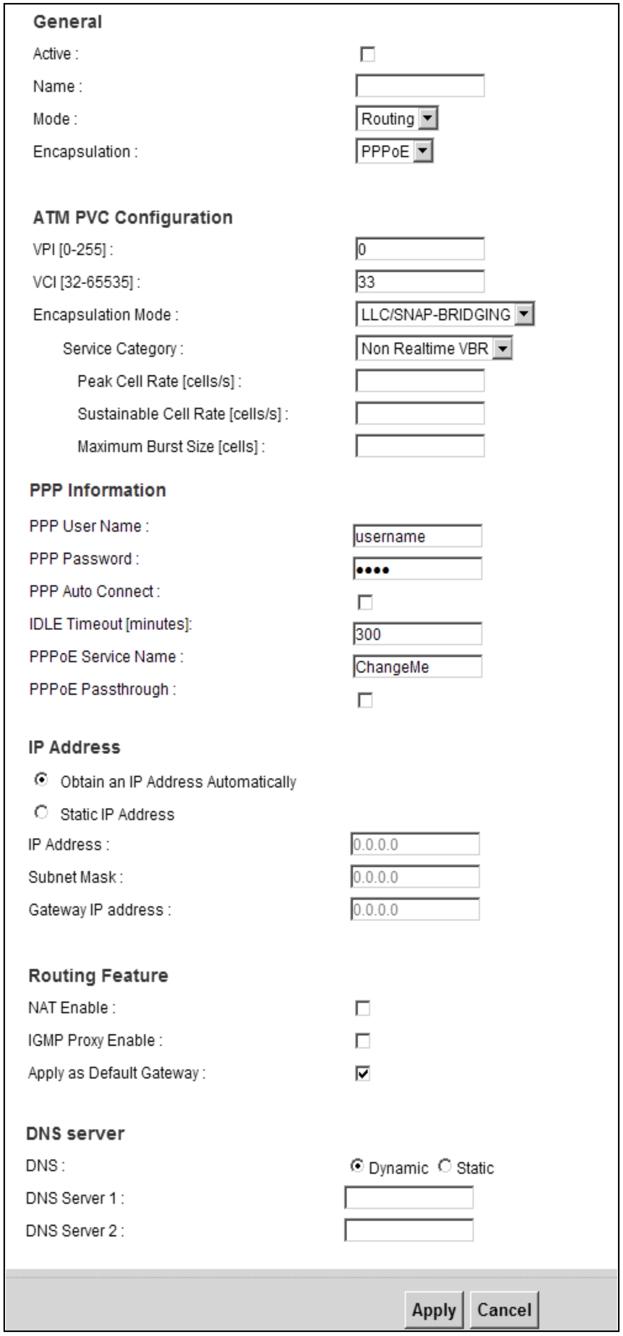
LABEL	DESCRIPTION
Add new WAN interface	Click this button to create a new connection.
#	This is the index number of the entry.
Status	This is the status of the connection.
Name	This is the service name of the connection.
Encapsulation	This is the method of encapsulation used by this connection.
VPI/VCI	This is the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers configured for this WAN connection.
ATM QoS	This is the type of ATM QoS of the connection.
IGMP Proxy	This shows whether the ZyXEL Device act as an IGMP proxy on this connection.
NAT	This shows whether NAT is activated or not for this connection.
Default Gateway	This shows whether the ZyXEL Device use the WAN interface of this connection as the system default gateway.
Modify	Click the **Edit** icon to configure the WAN connection. Click the **Delete** icon to remove the WAN connection.

5.2.1 Add/Edit Broadband

Click **Add new WAN interface** in the **Broadband** screen or the **Edit** icon next to an existing WAN interface to configure a WAN connection. The screen differs according to the mode and encapsulation you choose.

This screen displays when you select the **Routing** mode and **PPPoE** encapsulation. The fields in the screen may differ depending on the type of encapsulation you use.

Figure 13 Broadband: Add/Edit: Routing Mode



General

Active : □

Name :

Mode : Routing

Encapsulation : PPPoE

ATM PVC Configuration

VPI [0-255] : 0

VCI [32-65535] : 33

Encapsulation Mode : LLC/SNAP-BRIDGING

Service Category : Non Realtime VBR

Peak Cell Rate [cells/s] :

Sustainable Cell Rate [cells/s] :

Maximum Burst Size [cells] :

PPP Information

PPP User Name : username

PPP Password : ●●●●

PPP Auto Connect : □

IDLE Timeout [minutes]: 300

PPPoE Service Name : ChangeMe

PPPoE Passthrough : □

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Gateway IP address : 0.0.0.0

Routing Feature

NAT Enable : □

IGMP Proxy Enable : □

Apply as Default Gateway : ☑

DNS server

DNS : ● Dynamic ○ Static

DNS Server 1 :

DNS Server 2 :

The following table describes the labels in this screen.

Table 6 Broadband: Add/Edit: Routing Mode

LABEL	DESCRIPTION
General	
Active	Select this to activate the WAN configuration settings.
Name	Specify a descriptive name of up to 15 alphanumeric characters for this connection.

Table 6 Broadband: Add/Edit: Routing Mode (continued)

LABEL	DESCRIPTION
Mode	Select **Routing** (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. This option is available only when you select **Routing** in the **Mode** field. The choices are **PPPoE**, **PPPoA**, **IPoE** and **IPoA**.
ATM PVC Configuration	
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
Encapsulation Mode	Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: • **LLC/SNAP-BRIDGING:** In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select **IPoE** or **PPPoE** in the Select DSL Link Type field. • **VC/MUX:** In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the ZyXEL Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload. • **LLC/ENCAPSULATION:** More than one protocol can be carried over the same VC. This is available only when you select **PPPoA** in the **Encapsulation** field. • **LLC/SNAP-ROUTING:** In LCC encapsulation, an IEEE 802.2 Logical Link Control (LLC) header is prefixed to each routed PDU to identify the PDUs. The LCC header can be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. This is available only when you select **IPoA** in the **Encapsulation** field.
Service Category	Select **UBR Without PCR** or **UBR With PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.This field is not available when you select **UBR Without PCR**.

Table 6 Broadband: Add/Edit: Routing Mode (continued)

LABEL	DESCRIPTION
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
PPP Information	This is available only when you select **PPPoE** or **PPPoA** in the **Mode** field.
PPP Username	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
PPP Auto Connect	Select this option if you do not want the connection to time out.
IDLE Timeout	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server. This field is not configurable if you select **PPP Auto Connect**.
PPPoE Service Name	Enter the name of your PPPoE service here.
PPPoE Passthrough	This field is available when you select **PPPoE** encapsulation. In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
IP Address	This is available only when you select **IPoE** or **IPoA** in the **Mode** field.
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
IP Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the gateway IP address provided by your ISP.

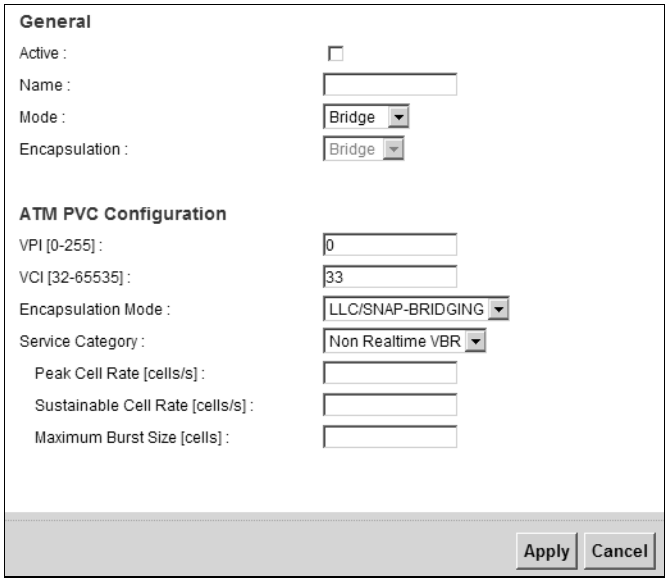
Table 6 Broadband: Add/Edit: Routing Mode (continued)

LABEL	DESCRIPTION
Routing Feature	
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Select this option to have the ZyXEL Device act as an IGMP proxy on this connection. This allows the ZyXEL Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the ZyXEL Device use the WAN interface of this connection as the system default gateway.
DNS Server	This is available only when you select **Apply as Default Gateway** in the **Routing Feature** field.
DNS	Select **Dynamic** if you want the ZyXEL Device use the DNS server addresses assigned by your ISP. Select **Static** if you want the ZyXEL Device use the DNS server addresses you configure manually.
DNS Server 1	Enter the first DNS server address assigned by the ISP.
DNS Server 2	Enter the second DNS server address assigned by the ISP.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to exit this screen without saving.

5.2.1.1 Bridge

This screen displays when you select the **Bridge** mode.

Figure 14 Broadband: Add/Edit: Bridge Mode



General

Active : □

Name :

Mode : Bridge

Encapsulation : Bridge

ATM PVC Configuration

VPI [0-255] : 0

VCI [32-65535] : 33

Encapsulation Mode : LLC/SNAP-BRIDGING

Service Category : Non Realtime VBR

Peak Cell Rate [cells/s] :

Sustainable Cell Rate [cells/s] :

Maximum Burst Size [cells] :

The following table describes the labels in this screen.

Table 7 Broadband: Add/Edit: Bridge Mode

LABEL	DESCRIPTION
General	
Active	Select this to activate the WAN configuration settings.
Name	Specify a descriptive name of up to 15 alphanumeric characters for this connection.
Mode	Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
Encapsulation	This field is not available if you select **Bridge** mode.
ATM PVC Configuration	
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
Encapsulation Mode	Select the method of multiplexing used by your ISP from the drop-down list box. Choices are: • **LLC/SNAP-BRIDGING:** In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. • **VC/MUX:** In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the ZyXEL Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload.
Service Category	Select **UBR Without PCR** or **UBR With PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.This field is not available when you select **UBR Without PCR**.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.

Table 7 Broadband: Add/Edit: Bridge Mode (continued)

LABEL	DESCRIPTION
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to exit this screen without saving.

5.3 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

5.3.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The ZyXEL Device supports the following methods.

5.3.1.1 PPP over Ethernet

The ZyXEL Device supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The PPPoE option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyXEL Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyXEL Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

5.3.1.2 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The ZyXEL Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (Digital Subscriber Line (DSL) Access Multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

5.3.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

5.3.3 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

5.3.4 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP.

IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **Gateway IP Address** fields are not applicable (N/A). If you have a static IP, then you only need to fill in the **IP Address** field and not the **Gateway IP Address** field.

5.3.5 NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

5.4 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

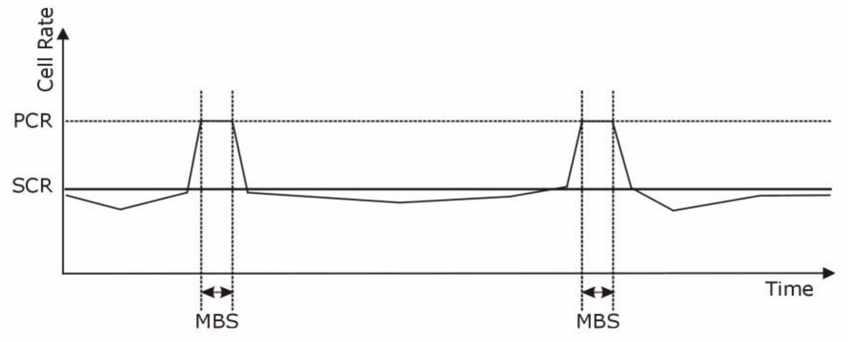
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 15 Example of Traffic Shaping



5.4.1 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

6

Wireless

6.1 Overview

This chapter describes the ZyXEL Device's **Network Settings > Wireless** screens. Use these screens to set up your ZyXEL Device's wireless connection.

6.1.1 What You Can Do in this Chapter

This section describes the ZyXEL Device's **Wireless** screens. Use these screens to set up your ZyXEL Device's wireless connection.

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode (Section 6.2 on page 78).
- Use the **More AP** screen to set up multiple wireless networks on your ZyXEL Device (Section 6.3 on page 86).
- Use the **MAC Authentication** screen to allow or deny wireless clients based on their MAC addresses from connecting to the ZyXEL Device (Section 6.4 on page 88).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 6.5 on page 90).
- Use the **WMM** screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications (Section 6.6 on page 91).
- Use the **WDS** screen to set up a Wireless Distribution System, in which the ZyXEL Device acts as a bridge with other ZyXEL access points (Section 6.7 on page 92).
- Use the **Others** screen to configure wireless advanced features, such as the RTS/CTS Threshold (Section 6.8 on page 95).

6.1.2 What You Need to Know

Wireless Basics

“Wireless” is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

Finding Out More

See Section 6.9 on page 96 for advanced technical information on wireless networks.

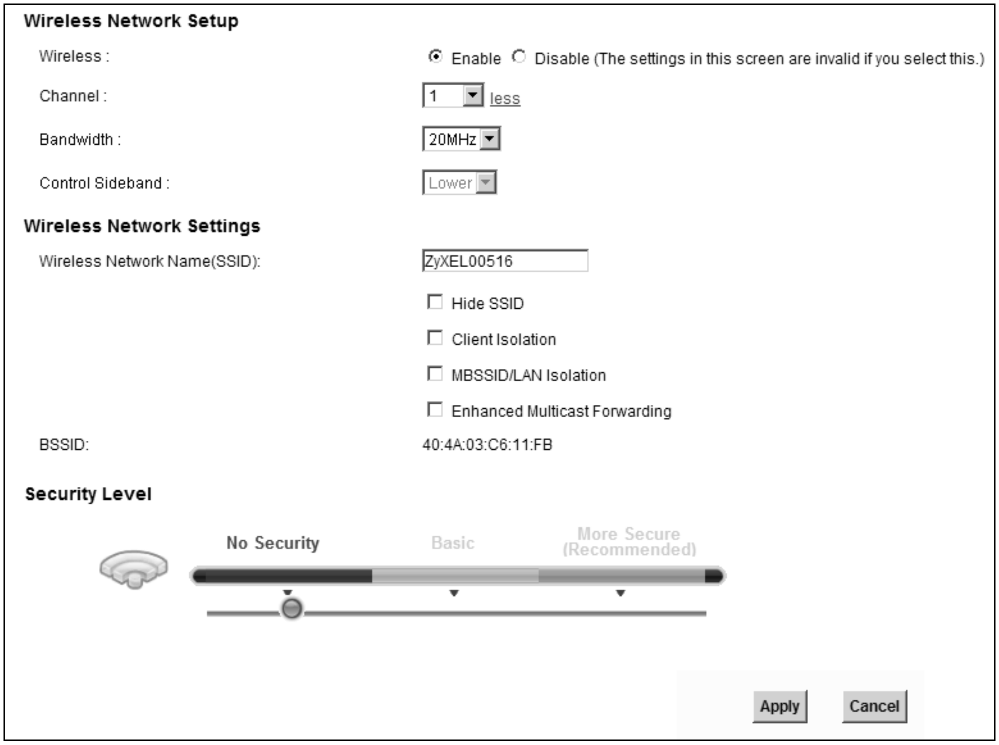
6.2 The General Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device’s SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device’s new settings.

Click **Network Settings** > **Wireless** to open the **General** screen.

Figure 16 Network Settings > Wireless > General



Wireless Network Setup

Wireless : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Channel : 1 less

Bandwidth : 20MHz

Control Sideband : Lower

Wireless Network Settings

Wireless Network Name(SSID): ZyXEL00516

□ Hide SSID

□ Client Isolation

□ MBSSID/LAN Isolation

□ Enhanced Multicast Forwarding

BSSID: 40:4A:03:C6:11:FB

Security Level

The following table describes the general wireless LAN labels in this screen.

Table 8 Network Settings > Wireless > General

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	You can **Enable** or **Disable** the wireless LAN in this field.
Channel	Set the channel depending on your particular region. Select a channel or use **Auto** to have the ZyXEL Device automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the ZyXEL Device is currently using then displays next to this field.
more.../less	Click **more...** to show more information. Click **less** to hide them.

Table 8 Network Settings > Wireless > General (continued)

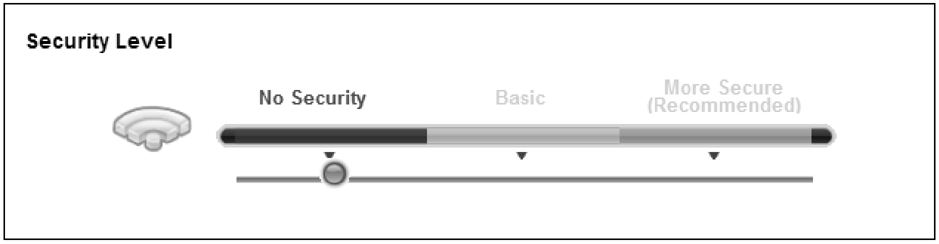
LABEL	DESCRIPTION
Bandwidth	Select whether the ZyXEL Device uses a wireless channel width of **20MHz** or **40MHz**. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.
Control Sideband	This is available for some regions when you select a specific channel and set the Bandwidth field to **40MHz**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Client Isolation	Select this check box to prevent the wireless client connected to the ZyXEL Device from communicating with other wireless clients.
MBSSID/LAN Isolation	Select this check box to prevent wireless devices of other BSSIDs/LAN to communicate with the wireless client.
Enhance Multicast Forwarding	Select this check box to allow the ZyXEL Device to convert wireless multicast traffic into wireless unicast traffic.
Security Level	
Security Mode	Select **Basic (WEP)** or **More Secure (WPA(2)-PSK, WPA(2))** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the ZyXEL Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about this field.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.2.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption or authentication.

Note: If you do not enable any wireless security on your ZyXEL Device, your network is accessible to any wireless networking device that is within range.

Figure 17 Wireless > General: No Security



The following table describes the labels in this screen.

Table 9 Wireless > General: No Security

LABEL	DESCRIPTION
Security Level	Choose **No Security** from the drop-down list box.

6.2.2 Basic (WEP Encryption)

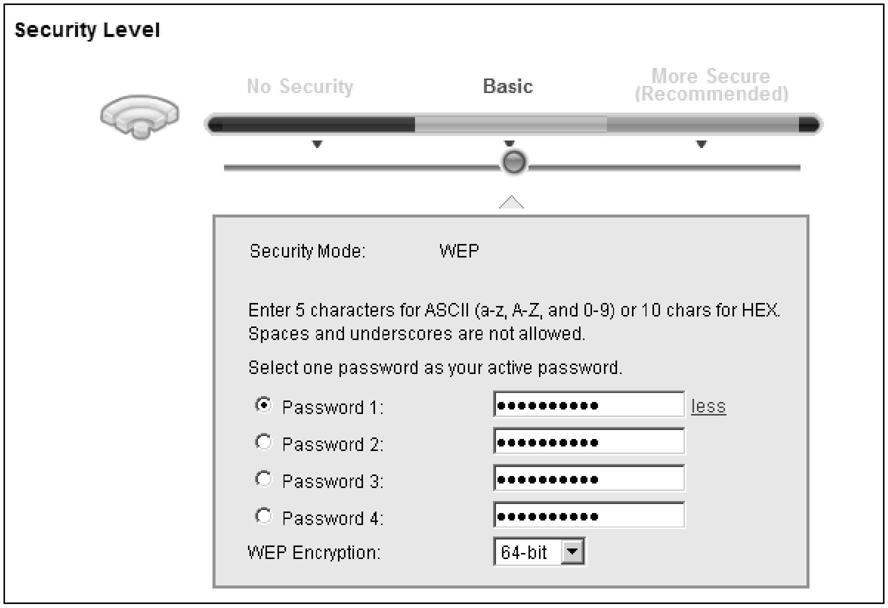
WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

Note: WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. For example, use WPA-PSK or WPA2-PSK if all your wireless devices support it, or use WPA or WPA2 if your wireless devices support it and you have a RADIUS server. If your wireless devices support nothing stronger than WEP, use the highest encryption level available.

Your ZyXEL Device allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption, click **Network Settings** > **Wireless** to display the **General** screen, then select **Basic** as the security level.

Figure 18 Wireless > General: Basic (WEP)



Security Mode: WEP

Enter 5 characters for ASCII (a-z, A-Z, and 0-9) or 10 chars for HEX. Spaces and underscores are not allowed.

Select one password as your active password.

● Password 1: ●●●●●●●●●●● less

○ Password 2: ●●●●●●●●●●●

○ Password 3: ●●●●●●●●●●●

○ Password 4: ●●●●●●●●●●●

WEP Encryption: 64-bit

The following table describes the labels in this screen.

Table 10 Wireless > General: Basic (WEP)

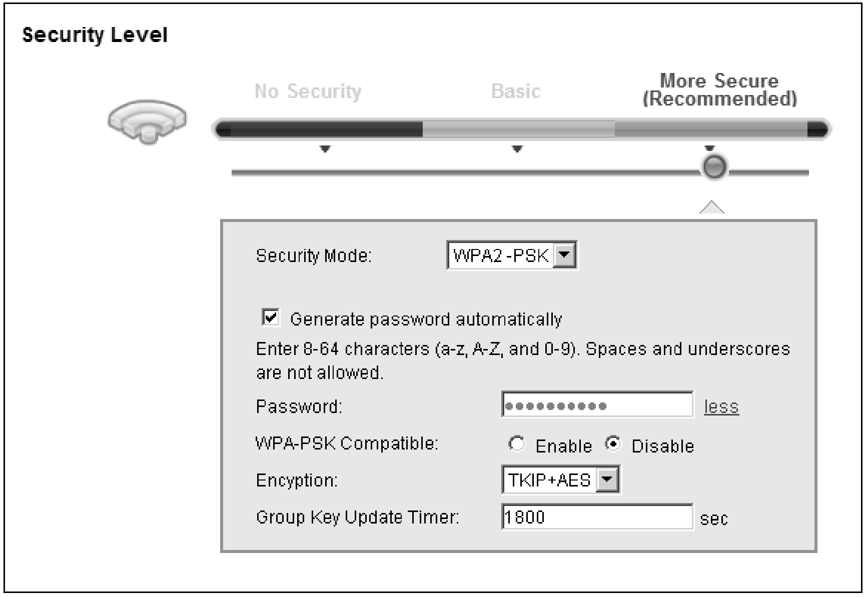
LABEL	DESCRIPTION
Security Level	Select **Basic** to enable WEP data encryption.
more.../less	Click **more...** to show more fields in this section. Click **less** to hide them.
Password 1~4	The password (WEP keys) are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same password (WEP key) for data transmission. If you chose **64-bit** WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit** WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one password, only one password can be activated at any one time. The default password is **Passowrd 1**.
WEP Encryption	Select **64-bits** or **128-bits**. This dictates the length of the security key that the network is going to use.

6.2.3 More Secure (WPA(2)-PSK)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the ZyXEL Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be.

Click **Network Settings** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 19 Wireless > General: More Secure: WPA(2)-PSK



Security Mode: WPA2-PSK

☑ Generate password automatically

Enter 8-64 characters (a-z, A-Z, and 0-9). Spaces and underscores are not allowed.

Password: ●●●●●●●●●●

WPA-PSK Compatible: ○ Enable ● Disable

Encyption: TKIP+AES

Group Key Update Timer: 1800 sec

The following table describes the labels in this screen.

Table 11 Wireless > General: More Secure: WPA(2)-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Select **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
Generate password automatically	Select this option to have the ZyXEL Device automatically generate a password. The password field will not be configurable when you select this option.
Password	The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 64 case-sensitive keyboard characters.
more.../less	Click **more...** to show more fields in this section. Click **less** to hide them.

Table 11 Wireless > General: More Secure: WPA(2)-PSK (continued)

LABEL	DESCRIPTION
WPA-PSK Compatible	This field appears when you choose **WPA-PSK2** as the **Security Mode**. Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your ZyXEL Device. The ZyXEL Device supports WPA-PSK and WPA2-PSK simultaneously.
Encryption	Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption. Select **TKIP** if your wireless clients can all use TKIP. Select **AES** if your wireless clients can all use AES. Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients.

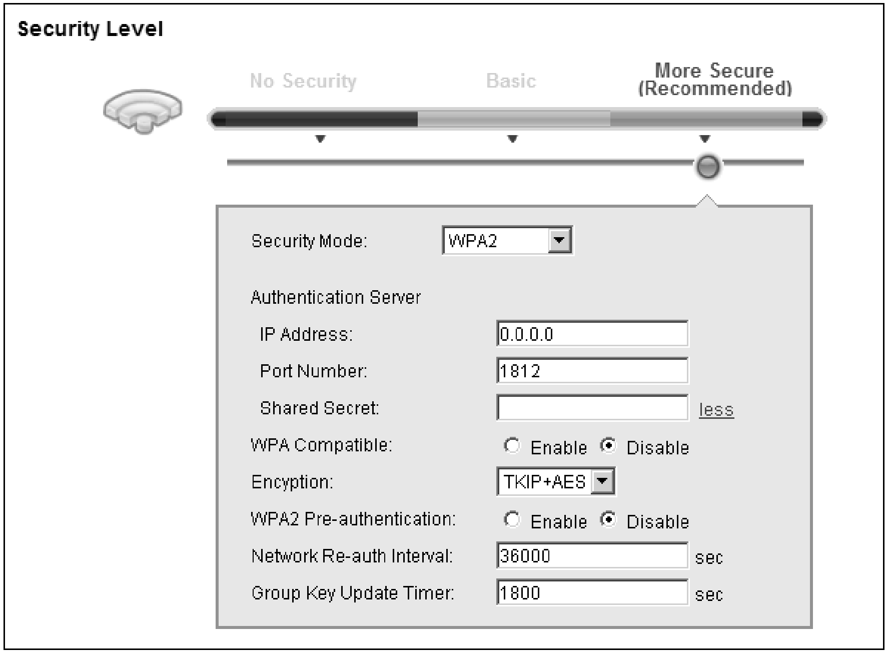
6.2.4 WPA(2) Authentication

The WPA2 security mode is currently the most robust form of encryption for wireless networks. It requires a RADIUS server to authenticate user credentials and is a full implementation the security protocol. Use this security option for maximum protection of your network. However, it is the least backwards compatible with older devices.

The WPA security mode is a security subset of WPA2. It requires the presence of a RADIUS server on your network in order to validate user credentials. This encryption standard is slightly older than WPA2 and therefore is more compatible with older devices.

Click **Network Settings** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA** or **WPA2** from the **Security Mode** list.

Figure 20 Wireless > General: More Secure: WPA(2)



Security Mode: WPA2

Authentication Server

IP Address: 0.0.0.0

Port Number: 1812

Shared Secret: less

WPA Compatible: ○ Enable ● Disable

Encyption: TKIP+AES

WPA2 Pre-authentication: ○ Enable ● Disable

Network Re-auth Interval: 36000 sec

Group Key Update Timer: 1800 sec

The following table describes the labels in this screen.

Table 12 Wireless > General: More Secure: WPA(2)

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Choose **WPA** or **WPA2** from the drop-down list box.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
more.../less	Click **more...** to show more fields in this section. Click **less** to hide them.
WPA Compatible	This field is only available for WPA2. Select this if you want the ZyXEL Device to support WPA and WPA2 simultaneously.

Table 12 Wireless > General: More Secure: WPA(2) (continued)

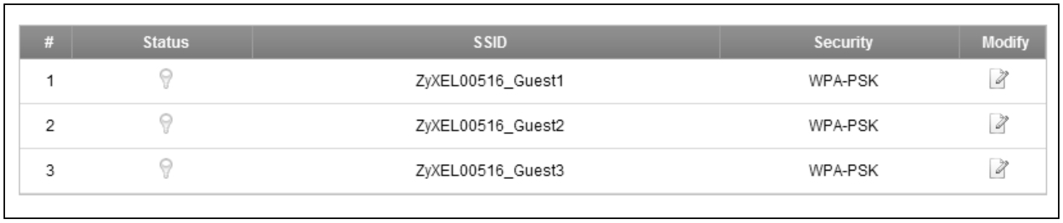
LABEL	DESCRIPTION
Encryption	Select the encryption type (**TKIP**, **AES** or **TKIP+AES**) for data encryption. Select **TKIP** if your wireless clients can all use TKIP. Select **AES** if your wireless clients can all use AES. Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES.
WPA2 Pre-Authentication	This field is available only when you select **WPA2**. Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Select **Enabled** to turn on preauthentication in WAP2. Otherwise, select **Disabled**.
Network Re-auth Interval	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients.

6.3 The More AP Screen

This screen allows you to enable and configure multiple Basic Service Sets (BSSs) on the ZyXEL Device.

Click **Network Settings > Wireless** > **More AP**. The following screen displays.

Figure 21 Network Settings > Wireless > More AP



#	Status	SSID	Security	Modify
1	○	ZyXEL00516_Guest1	WPA-PSK	✎
2	○	ZyXEL00516_Guest2	WPA-PSK	✎
3	○	ZyXEL00516_Guest3	WPA-PSK	✎

The following table describes the labels in this screen.

Table 13 Network Settings > Wireless > More AP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active. A gray bulb signifies that this SSID is not active.

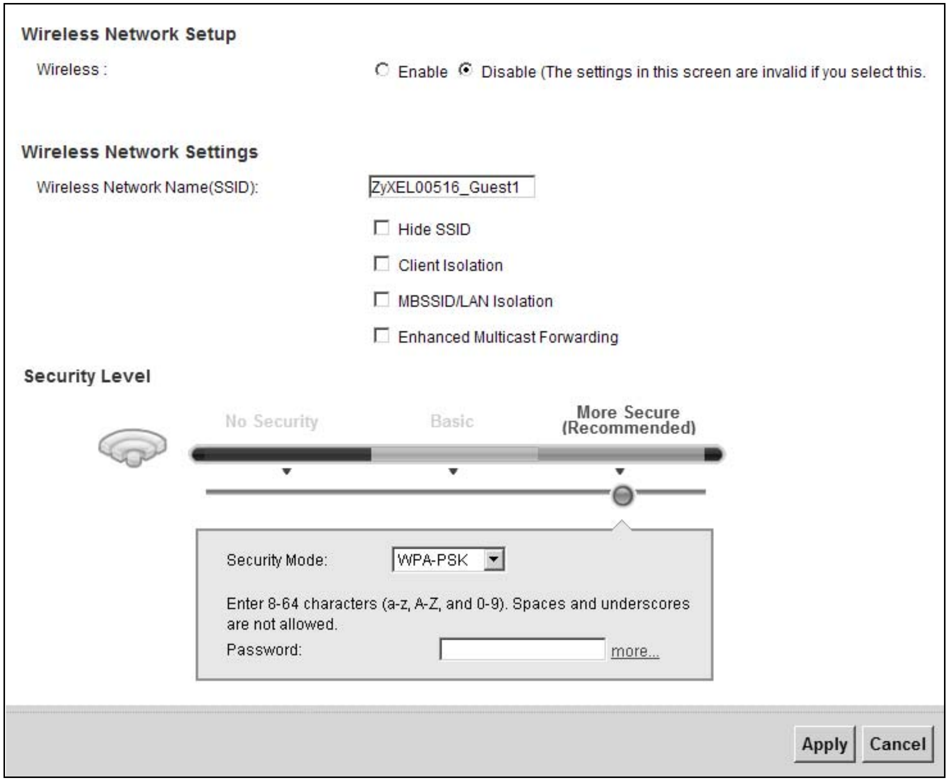
Table 13 Network Settings > Wireless > More AP (continued)

LABEL	DESCRIPTION
SSID	An SSID profile is the set of parameters relating to one of the ZyXEL Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the **Edit** icon to configure the SSID profile.

6.3.1 Edit More AP

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 22 More AP: Edit



Wireless Network Setup

Wireless : ○ Enable ● Disable (The settings in this screen are invalid if you select this.

Wireless Network Settings

Wireless Network Name(SSID): ZyXEL00516_Guest1

□ Hide SSID

□ Client Isolation

□ MBSSID/LAN Isolation

□ Enhanced Multicast Forwarding

Security Level

Security Mode: WPA-PSK

Enter 8-64 characters (a-z, A-Z, and 0-9). Spaces and underscores are not allowed.

Password:

The following table describes the fields in this screen.

Table 14 More AP: Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	You can **Enable** or **Disable** the wireless LAN in this field.

Table 14 More AP: Edit (continued)

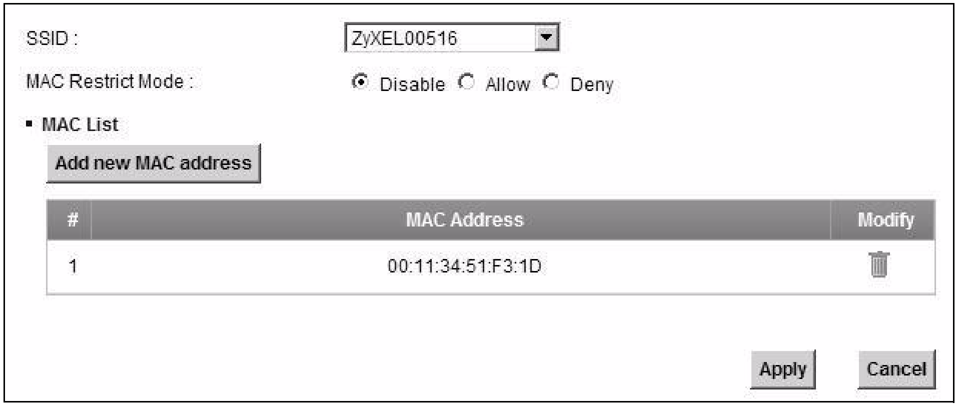
LABEL	DESCRIPTION
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Client Isolation	Select this check box to prevent the wireless client connected to the ZyXEL Device from communicating with other wireless clients.
MBSSID/LAN Isolation	Select this check box to prevent wireless devices of other BSSIDs/ LAN to communicate with the wireless client.
Enhance Multicast Forwarding	Select this check box to allow the ZyXEL Device to convert wireless multicast traffic into wireless unicast traffic.
Security Level	
Security Mode	Select **Basic (WEP)** or **More Secure (WPA(2)-PSK, WPA(2))** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the ZyXEL Device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See Section 6.2.1 on page 81 for more details about this field.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

6.4 MAC Authentication

This screen allows you to configure the ZyXEL Device to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the ZyXEL Device **(Deny)**. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Use this screen to view your ZyXEL Device's MAC filter settings and add new MAC filter rules. Click **Wireless > MAC Authentication**. The screen appears as shown.

Figure 23 Wireless > MAC Authentication



SSID : ZyXEL00516

MAC Restrict Mode : ● Disable ○ Allow ○ Deny

- MAC List

#	MAC Address	Modify
1	00:11:34:51:F3:1D	🗑

The following table describes the labels in this screen.

Table 15 Wireless > MAC Authentication

LABEL	DESCRIPTION
SSID	Select the SSID that you want to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Disable** to turn off MAC filtering. Select **Deny** to block access to the ZyXEL Device. MAC addresses not listed will be allowed to access the ZyXEL Device. Select **Allow** to permit access to the ZyXEL Device. MAC addresses not listed will be denied access to the ZyXEL Device.
Add new MAC address	Click this if you want to add a new MAC address entry to the MAC filter list below. Enter the MAC addresses of the wireless devices that are allowed or denied access to the ZyXEL Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
#	This is the index number of the entry.
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the ZyXEL Device.
Modify	Click the **Delete** icon to delete the entry.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

6.5 The WPS Screen

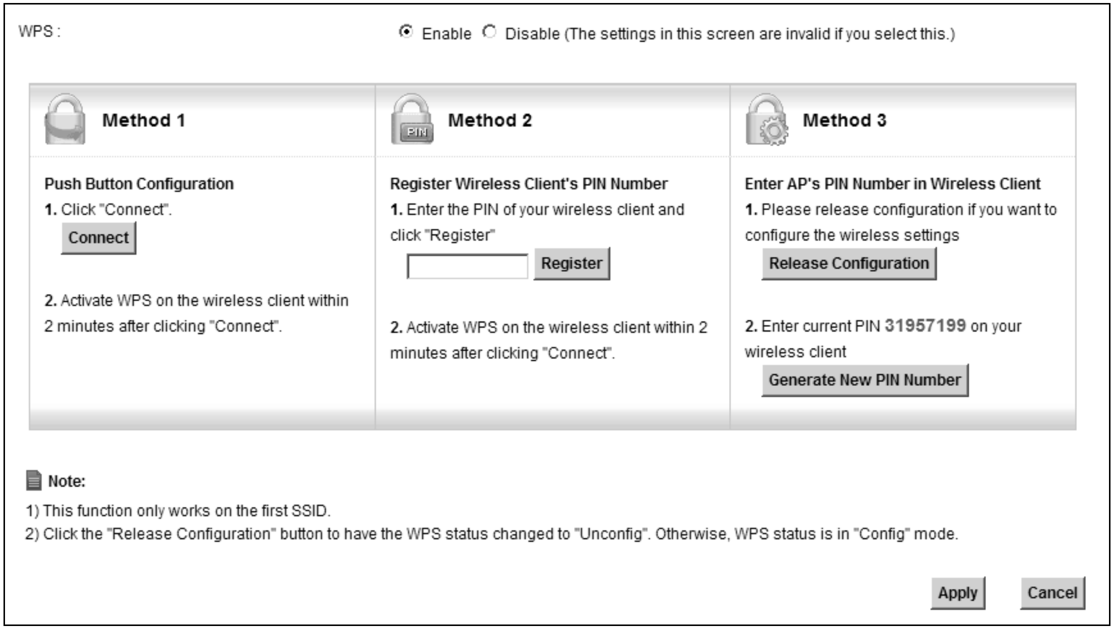
Use this screen to configure WiFi Protected Setup (WPS) on your ZyXEL Device.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See Section 6.9.8.3 on page 107 for more information about WPS.

Note: The ZyXEL Device applies the security settings of the **SSID1** profile (see Section 6.2 on page 78). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA-PSK**, **WPA2-PSK** or **No Security**.

Click **Network Settings > Wireless > WPS**. The following screen displays. Select **Enable** and click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 24 Network Settings > Wireless > WPS



WPS : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Method 1

Push Button Configuration

1. Click "Connect".

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 2

Register Wireless Client's PIN Number

1. Enter the PIN of your wireless client and click "Register"

2. Activate WPS on the wireless client within 2 minutes after clicking "Connect".

Method 3

Enter AP's PIN Number in Wireless Client

1. Please release configuration if you want to configure the wireless settings

2. Enter current PIN **31957199** on your wireless client

Note:

1) This function only works on the first SSID.

2) Click the "Release Configuration" button to have the WPS status changed to "Unconfig". Otherwise, WPS status is in "Config" mode.

The following table describes the labels in this screen.

Table 16 Network Settings > Wireless > WPS

LABEL	DESCRIPTION
Enable WPS	Select **Enable** to activate WPS on the ZyXEL Device.
Method 1	Use this section to set up a WPS wireless network using Push Button Configuration (PBC).

Table 16 Network Settings > Wireless > WPS (continued)

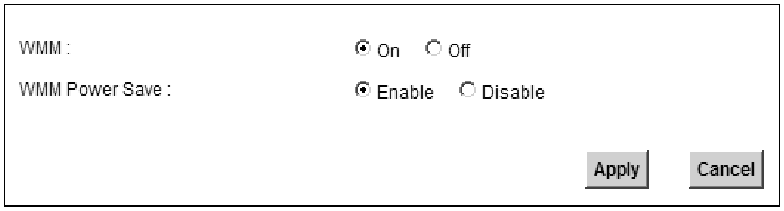
LABEL	DESCRIPTION
Connect	Click this button to add another WPS-enabled wireless device (within wireless range of the ZyXEL Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **Connect** button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Method 2	Use this section to set up a WPS wireless network by entering the PIN of the client into the ZyXEL Device.
Register	Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the ZyXEL Device.
Method 3	Use this section to set up a WPS wireless network by entering the PIN of the ZyXEL Device into the client.
Release Configuration	The default WPS status is configured. Click this button to remove all configured wireless and wireless security settings for WPS connections on the ZyXEL Device.
Generate New PIN Number	The PIN (Personal Identification Number) of the ZyXEL Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method. Click the **Generate New PIN Number** button to have the ZyXEL Device create a new PIN.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.6 The WMM Screen

Use this screen to enable Wi-Fi MultiMedia (WMM) and WMM Power Save in wireless networks for multimedia applications.

Click **Network Settings > Wireless > WMM**. The following screen displays.

Figure 25 Network Settings > Wireless > WMM



WMM : ● On ○ Off

WMM Power Save : ● Enable ○ Disable

The following table describes the labels in this screen.

Table 17 Network Settings > Wireless > WMM

LABEL	DESCRIPTION
WMM	Select **On** to have the ZyXEL Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
WMM Power Save	Select this option to extend the battery life of your mobile devices (especially useful for small devices that are running multimedia applications). The ZyXEL Device goes to sleep mode to save power when it is not transmitting data. The AP buffers the packets sent to the ZyXEL Device until the ZyXEL Device "wakes up". The ZyXEL Device wakes up periodically to check for incoming data. Note: Note: This works only if the wireless device to which the ZyXEL Device is connected also supports this feature.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.7 The WDS Screen

An AP using the Wireless Distribution System (WDS) can function as a wireless network bridge allowing you to wirelessly connect two wired network segments. The **WDS** screen allows you to configure the ZyXEL Device to connect to two or more APs wirelessly when WDS is enabled.

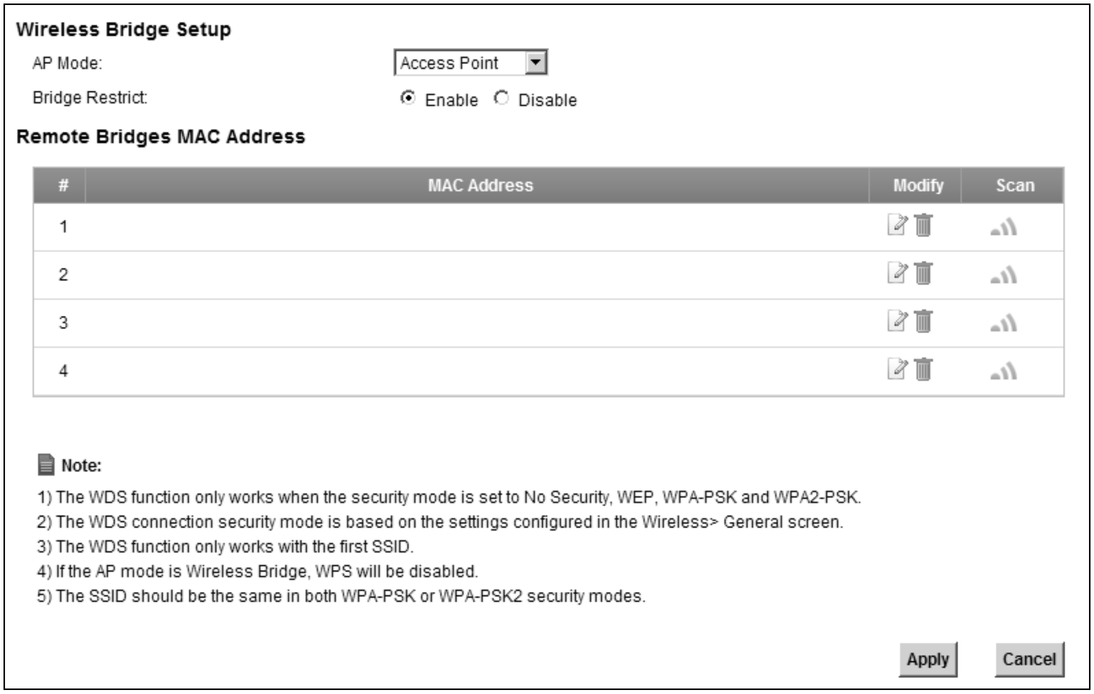
Use this screen to set up your WDS (Wireless Distribution System) links between the ZyXEL Device and other wireless APs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between devices is made.

Note: WDS security is independent of the security settings between the ZyXEL Device and any wireless clients.

Note: At the time of writing, WDS is compatible with other ZyXEL APs only. Not all models support WDS links. Check your other AP's documentation.

Click **Network Settings > Wireless > WDS**. The following screen displays.

Figure 26 Network Settings > Wireless > WDS



Wireless Bridge Setup

AP Mode: Access Point

Bridge Restrict: ● Enable ○ Disable

Remote Bridges MAC Address

#	MAC Address	Modify	Scan
1			
2			
3			
4			

Note:

1) The WDS function only works when the security mode is set to No Security, WEP, WPA-PSK and WPA2-PSK.
2) The WDS connection security mode is based on the settings configured in the Wireless> General screen.
3) The WDS function only works with the first SSID.
4) If the AP mode is Wireless Bridge, WPS will be disabled.
5) The SSID should be the same in both WPA-PSK or WPA-PSK2 security modes.

The following table describes the labels in this screen.

Table 18 Network Settings > Wireless > WDS

LABEL	DESCRIPTION
Wireless Bridge Setup	
AP Mode	Select the operating mode for your ZyXEL Device. • **Access Point** - The ZyXEL Device functions as a bridge and access point simultaneously. • **Wireless Bridge** - The ZyXEL Device acts as a wireless network bridge and establishes wireless links with other APs. In this mode, clients cannot connect to the ZyXEL Device wirelessly.
Bridge Restrict	This field is available only when you set operating mode to **Access Point**. Select **Enabled** to turn on WDS and enter the peer device's MAC address manually in the table below. Select **Disable** to turn off WDS.
Remote Bridge MAC Address	You can enter the MAC address of the peer device by clicking the **Edit** icon under **Modify**.
#	This is the index number of the entry.
MAC Address	This shows the MAC address of the peer device. You can connect to up to 4 peer devices.
Modify	Click the **Edit** icon and type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc). Click the **Delete** icon to remove this entry.

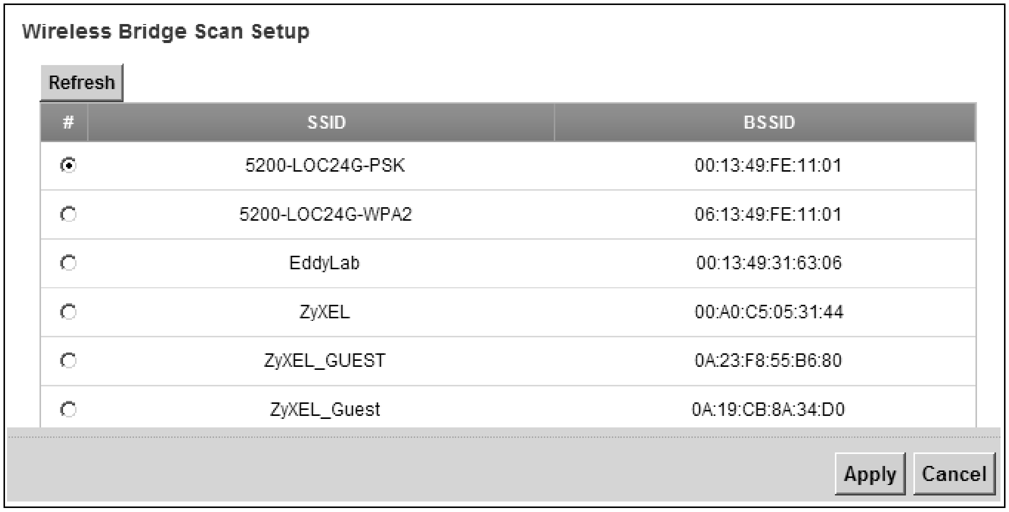
Table 18 Network Settings > Wireless > WDS (continued)

LABEL	DESCRIPTION
Scan	Click the **Scan** icon to search and display the available APs within range.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.7.1 WDS Scan

You can click the **Scan** icon in **Wireless > WDS** to have the ZyXEL Device automatically search and display the available APs within range. Select an AP and click **Apply** to have the ZyXEL Device establish a wireless link with the selected wireless device.

Figure 27 WDS: Scan



Wireless Bridge Scan Setup

#	SSID	BSSID
●	5200-LOC24G-PSK	00:13:49:FE:11:01
○	5200-LOC24G-WPA2	06:13:49:FE:11:01
○	EddyLab	00:13:49:31:63:06
○	ZyXEL	00:A0:C5:05:31:44
○	ZyXEL_GUEST	0A:23:F8:55:B6:80
○	ZyXEL_Guest	0A:19:CB:8A:34:D0

The following table describes the labels in this screen.

Table 19 WDS: Scan

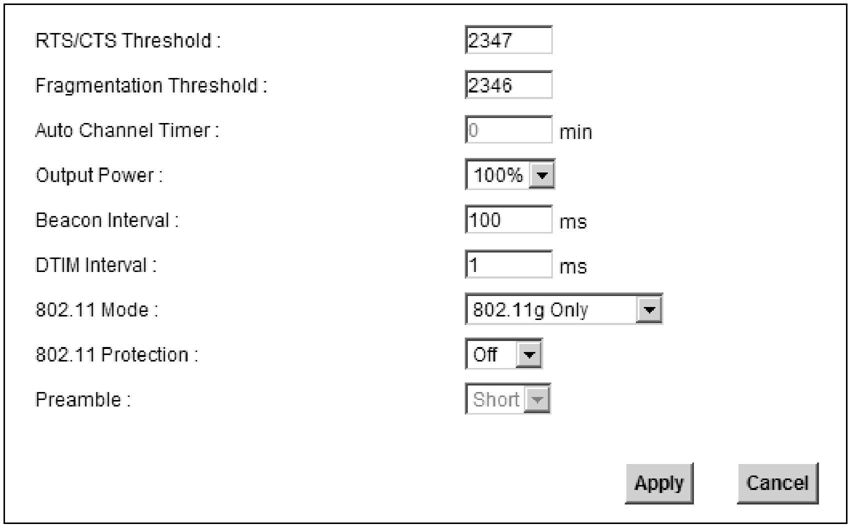
LABEL	DESCRIPTION
Wireless Bridge Scan Setup	
Refresh	Click **Refresh** to update the table.
#	This is the index number of the entry.
SSID	This shows the SSID of the available wireless device within range.
BSSID	This shows the MAC address of the available wireless device within range.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.8 The Wireless Others Screen

Use this screen to configure advanced wireless settings. Click **Network Settings > Wireless > Others**. The screen appears as shown.

See Section 6.9.2 on page 98 for detailed definitions of the terms listed in this screen.

Figure 28 Network Settings > Wireless > Others



RTS/CTS Threshold : 2347

Fragmentation Threshold : 2346

Auto Channel Timer : 0 min

Output Power : 100%

Beacon Interval : 100 ms

DTIM Interval : 1 ms

802.11 Mode : 802.11g Only

802.11 Protection : Off

Preamble : Short

The following table describes the labels in this screen.

Table 20 Network Settings > Wireless > Others

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2347.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.
Auto Channel Timer	If you set the channel to **Auto** in the **Network Settings > Wireless > General** screen, specify the interval in minutes for how often the ZyXEL Device scans for the best channel. Enter 0 to disable the periodical scan.
Output Power	Set the output power of the ZyXEL Device. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs. Select one of the following: **20%**, **40%**, **60%**, **80%** or **100%**.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from20ms to 1000ms. A high value helps save current consumption of the access point.

Table 20 Network Settings > Wireless > Others (continued)

LABEL	DESCRIPTION
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 100.
802.11 Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **802.11n Only** to allow only IEEE 802.11n compliant WLAN devices to associate with the ZyXEL Device. Select **802.11b/g Mixed** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced. Select **802.11b/g/n Mixed** to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
802.11 Protection	Enabling this feature can help prevent collisions in mixed-mode networks (networks with both IEEE 802.11b and IEEE 802.11g traffic). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11g performance. Select **Off** to disable 802.11 protection. The transmission rate of your ZyXEL Device might be reduced in a mixed-mode network. This field displays **Off** and is not configurable when you set **802.11 Mode** to **802.11b Only**.
Preamble	Select a preamble type from the drop-down list box. Choices are **Long** or **Short**. See the Section 6.9.9 on page 111 for more information. This field is configurable only when you set 802.11 Mode to **802.11b**.
Back	Click this to return to the previous screen without saving.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.9 Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

6.9.1 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

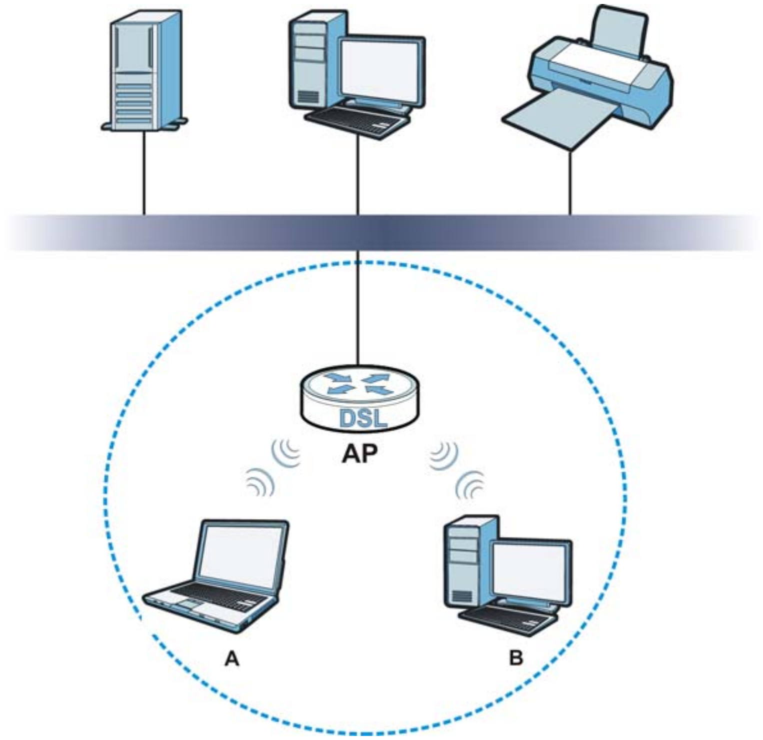
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 29 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your ZyXEL Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentifier.

- If two wireless networks overlap, they should use a different channel.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every device in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

6.9.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the ZyXEL Device’s Web Configurator.

Table 21 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other’s presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the ZyXEL Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the ZyXEL Device.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the ZyXEL Device does, it cannot communicate with the ZyXEL Device.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

6.9.3 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a “key” phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker’s software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it’s not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use “70dodchal71vanpoi” as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

6.9.3.1 SSID

Normally, the ZyXEL Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the ZyXEL Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

6.9.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the ZyXEL Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

6.9.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

[1] Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

[2] Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

6.9.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See Section 6.9.3.3 on page 100 for information about this.)

Table 22 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
↕	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the ZyXEL Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your ZyXEL Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the ZyXEL Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

6.9.4 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

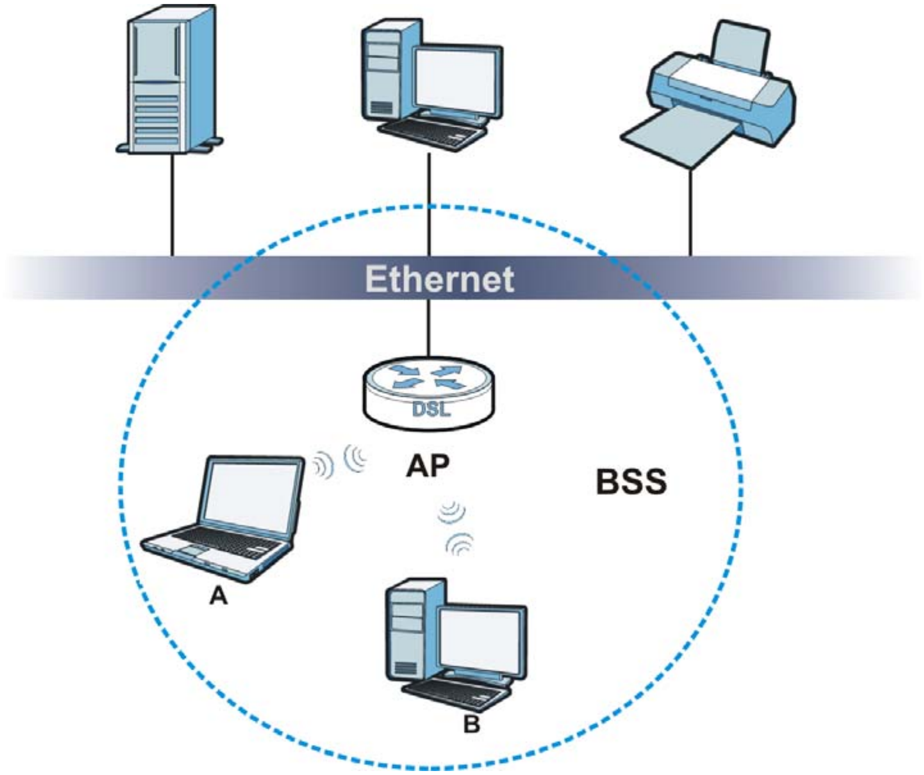
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

6.9.5 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 30 Basic Service set



6.9.6 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The ZyXEL Device’s MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

6.9.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other’s communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

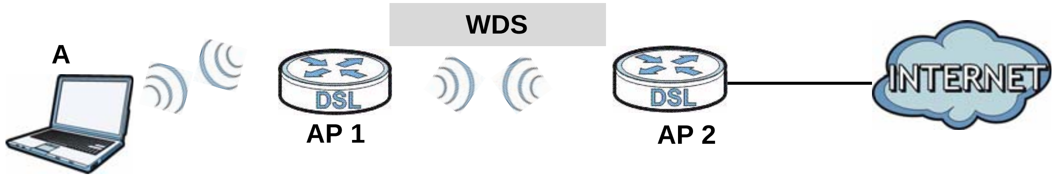
6.9.7 Wireless Distribution System (WDS)

The ZyXEL Device can act as a wireless network bridge and establish WDS (Wireless Distribution System) links with other APs. You need to know the MAC addresses of the APs you want to link to. Once the security settings of peer sides match one another, the connection between devices is made.

At the time of writing, WDS security is compatible with other ZyXEL access points only. Refer to your other access point's documentation for details.

The following figure illustrates how WDS link works between APs. Notebook computer **A** is a wireless client connecting to access point **AP 1**. **AP 1** has no wired Internet connection, but it can establish a WDS link with access point **AP 2**, which has a wired Internet connection. When **AP 1** has a WDS link with **AP 2**, the notebook computer can access the Internet through **AP 2**.

Figure 31 WDS Link Example



6.9.8 WiFi Protected Setup (WPS)

Your ZyXEL Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

6.9.8.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1 Ensure that the two devices you want to set up are within wireless range of one another.

2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the ZyXEL Device, see Section 6.6 on page 91).

3 Press the button on one of the devices (it doesn't matter which). For the ZyXEL Device you must press the WPS button for more than three seconds.

4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

6.9.8.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

1 Ensure WPS is enabled on both devices.

2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.

3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the ZyXEL Device, see Section 6.5 on page 90).

4 Enter the client's PIN in the AP's configuration interface.

5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.

6 Start WPS on both devices within two minutes.

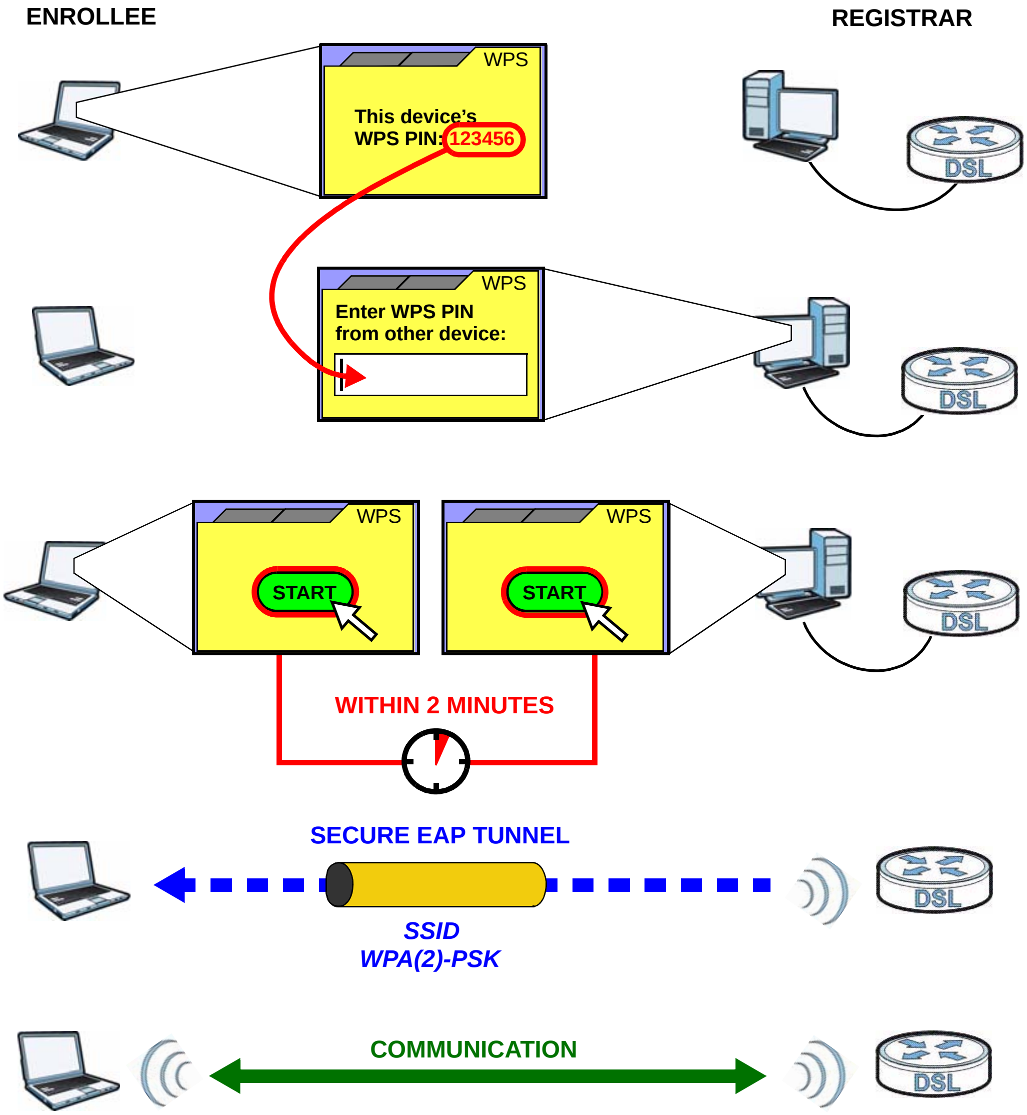
7 Use the configuration utility to activate WPS, not the push-button on the device itself.

8 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 32 Example WPS Process: PIN Method

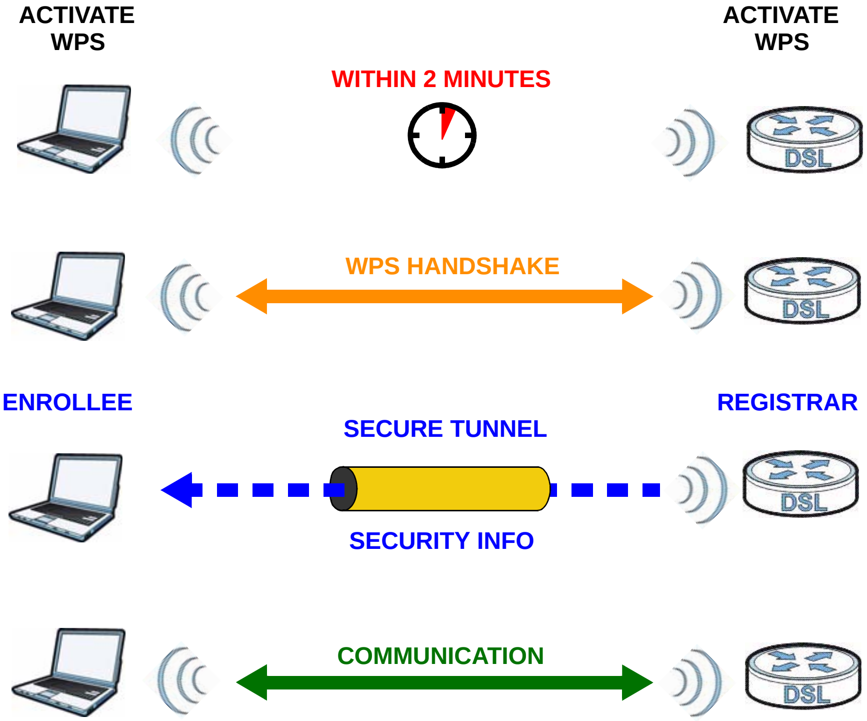


6.9.8.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 33 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

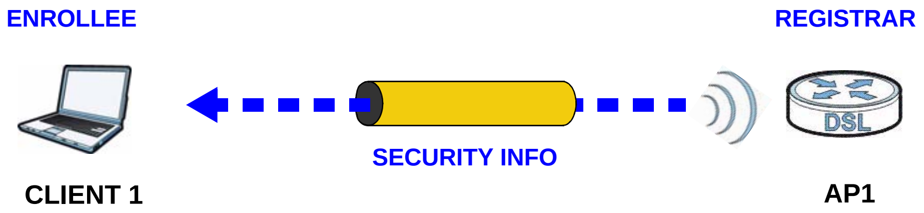
By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

6.9.8.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

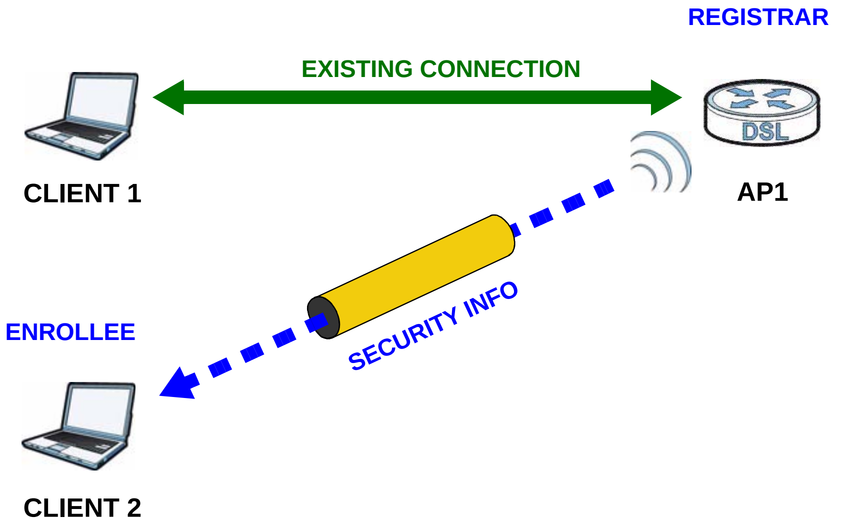
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 34 WPS: Example Network Step 1



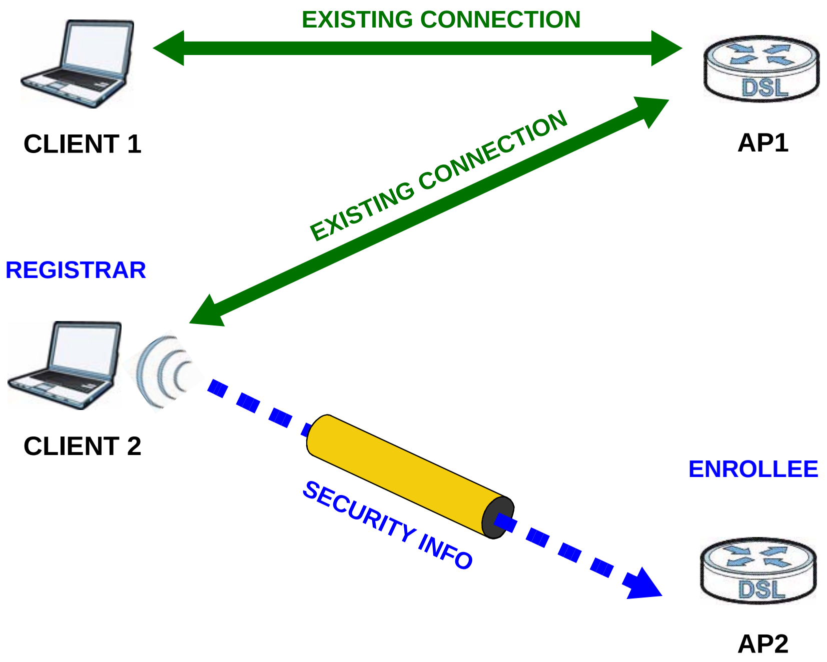
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 35 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 36 WPS: Example Network Step 3



6.9.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

6.9.9 Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the ZyXEL Device uses long preamble.

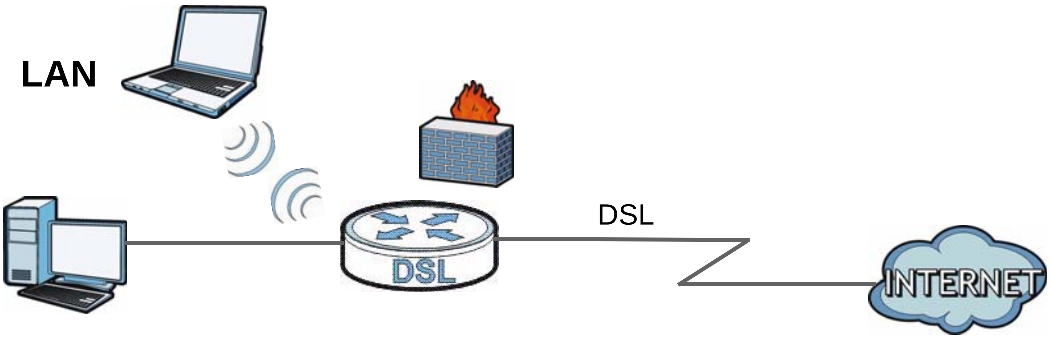
Note: The wireless devices MUST use the same preamble mode in order to communicate.

Home Networking

7.1 Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is usually located in one immediate area such as a building or floor of a building.

Use the LAN screens to help you configure a LAN DHCP server and manage IP addresses.



7.1.1 What You Can Do in this Chapter

- Use the **LAN Setup** screen to set the LAN IP address, subnet mask, and DHCP settings of your ZyXEL device (Section 7.2 on page 116).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 7.3 on page 118).
- Use the **UPnP** screen to enable UPnP on the ZyXEL Device (Section 7.4 on page 119).

7.1.2 What You Need To Know

7.1.2.1 About LAN

IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet Mask

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your ZyXEL Device an IP address, subnet mask, DNS and other routing information when it's turned on.

DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a networking device before you can access it.

7.1.2.2 About UPnP

Identifying UPnP Devices

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the Chapter 8 on page 133 for more information on NAT.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyXEL Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See Section 7.5 on page 120 for examples of installing and using UPnP.

Finding Out More

See Section 7.7 on page 128 for technical background information on LANs.

7.1.3 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

7.2 The LAN Setup Screen

Use this screen to set the Local Area Network IP address and subnet mask of your ZyXEL Device. Click **Network Settings > Home Networking** to open the **LAN Setup** screen.

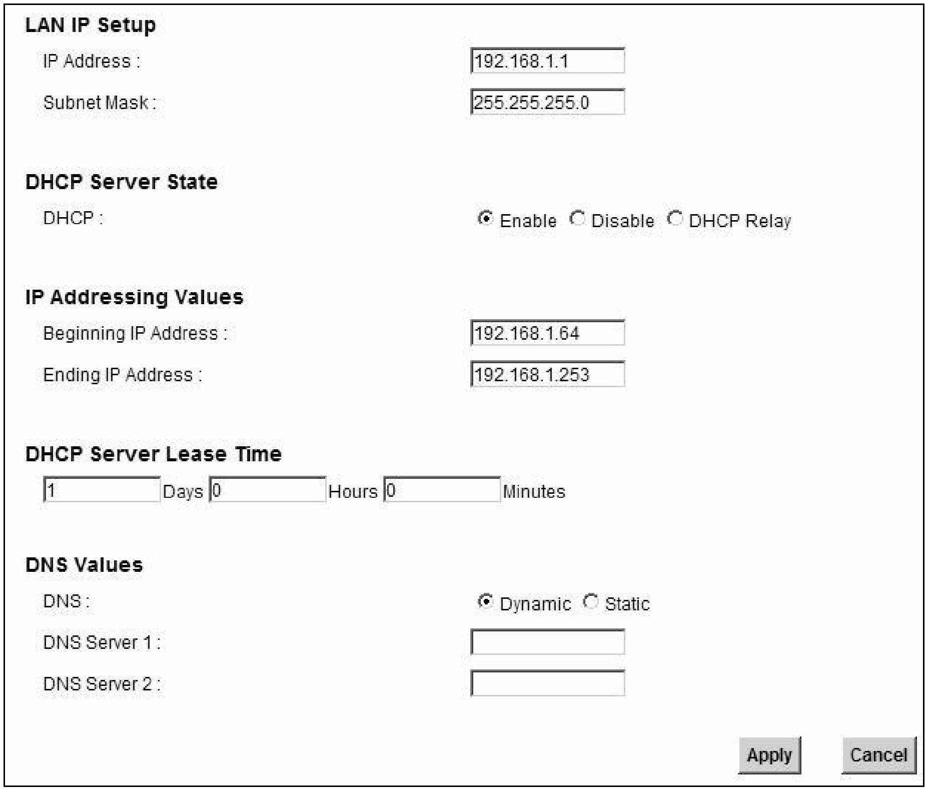
Follow these steps to configure your LAN settings.

1 Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your ZyXEL Device.

2 Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.

3 Click **Apply** to save your settings.

Figure 37 Network Settings > Home Networking > LAN Setup



LAN IP Setup

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

DHCP Server State

DHCP : ● Enable ○ Disable ○ DHCP Relay

IP Addressing Values

Beginning IP Address : 192.168.1.64

Ending IP Address : 192.168.1.253

DHCP Server Lease Time

1 Days 0 Hours 0 Minutes

DNS Values

DNS : ● Dynamic ○ Static

DNS Server 1 :

DNS Server 2 :

The following table describes the fields in this screen.

Table 23 Network Settings > Home Networking > LAN Setup

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your ZyXEL Device automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	
DHCP	Select **Enable** to have the ZyXEL Device act as a DHCP server or DHCP relay agent. Select **Disable** to stop the DHCP server on the ZyXEL Device. Select **DHCP Relay** to have the ZyXEL Device forward DHCP request to the DHCP server.
DHCP Relay Server Address	This field is only available when you select **DHCP Relay** in the **DHCP** field.
IP Address	Enter the IP address of the actual remote DHCP server in this field.
IP Addressing Values	This field is only available when you select **Enable** in the **DHCP** field.
Beginning IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
Ending IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
DHCP Server Lease Time	This is the period of time DHCP-assigned addresses is used. DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are “recycled” and made available for future reassignment to other systems. This field is only available when you select **Enable** in the **DHCP** field.
Days/Hours/ Minutes	Enter the lease time of the DHCP server.
DNS Values	This field is only available when you select **Enable** in the **DHCP** field.
DNS	Select the type of service that you are registered for from your Dynamic DNS service provider. Select **Dynamic** if you have the Dynamic DNS service. Select **Static** if you have the Static DNS service.
DNS Server 1 DNS Server 2	Enter the first and second DNS (Domain Name System) server IP address the ZyXEL Device passes to the DHCP clients.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

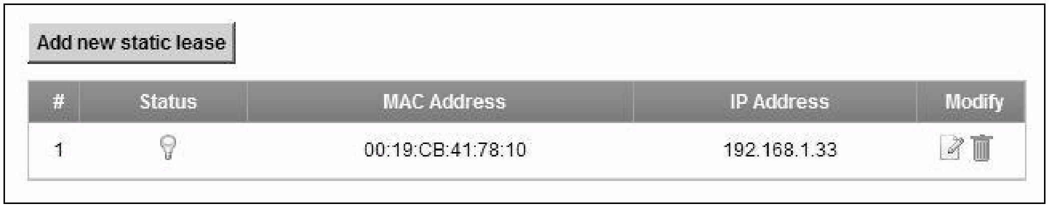
7.3 The Static DHCP Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Use this screen to change your ZyXEL Device's static DHCP settings. Click **Network Settings > Home Networking > Static DHCP** to open the following screen.

Figure 38 Network Settings > Home Networking > Static DHCP



#	Status	MAC Address	IP Address	Modify
1	💡	00:19:CB:41:78:10	192.168.1.33	✎ 🗑

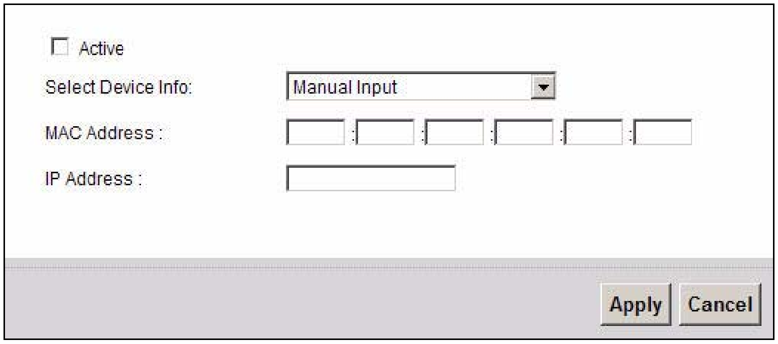
The following table describes the labels in this screen.

Table 24 Network Settings > Home Networking > Static DHCP

LABEL	DESCRIPTION
Add new static lease	Click this to add a new static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the ZyXEL Device.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Modify	Click the **Edit** icon to have the IP address field editable and change it. Click the **Delete** icon to delete a static DHCP entry. A window displays asking you to confirm that you want to delete the selected entry.

If you click **Add new static lease** in the **Static DHCP** screen or the Edit icon next to a static DHCP entry, the following screen displays.

Figure 39 Static DHCP: Add/Edit



□ Active

Select Device Info: Manual Input

MAC Address :

IP Address :

The following table describes the labels in this screen.

Table 25 Static DHCP: Add/Edit

LABEL	DESCRIPTION
Active	Select this check box to activate the Static DHCP function.
Select Device Info	If you select **Manual Input**, you can manually type in the MAC address and IP address of a computer on your LAN. You can also choose the name of a computer from the drop list and have the MAC Address and IP Address auto-detected.
MAC Address	If you select **Manual Input** in the **Select Device Info** field, enter the MAC address of a computer on your LAN.
IP Address	If you select **Manual Input** in the **Select Device Info** field, enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

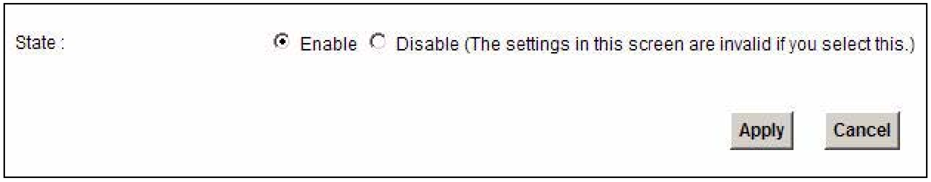
7.4 The UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

See page 114 for more information on UPnP.

Use the following screen to configure the UPnP settings on your ZyXEL Device. Click **Network Settings > Home Networking > UPnP** to display the screen shown next.

Figure 40 Network Settings > Home Networking > UPnP



State : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

The following table describes the labels in this screen.

Table 26 Network Settings > Home Networking > UPnP

LABEL	DESCRIPTION
State	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previous settings.

7.5 Installing UPnP in Windows Example

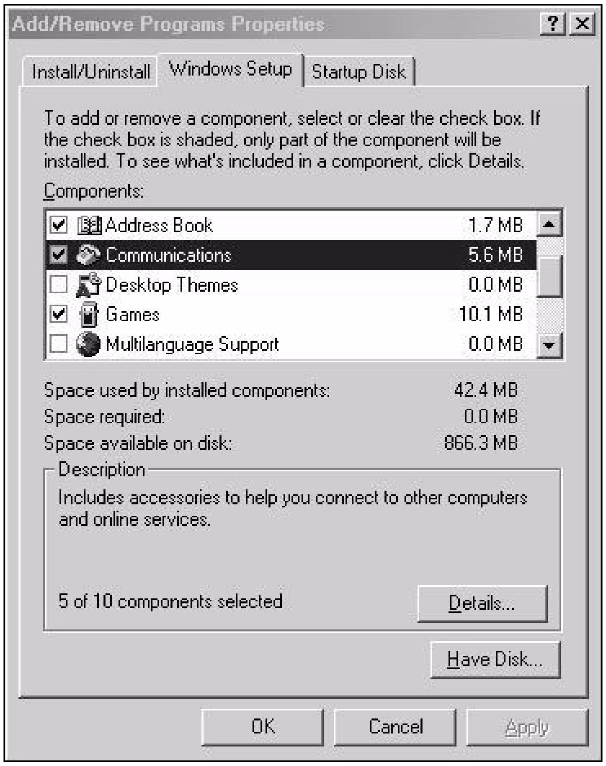
This section shows how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.



To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Address Book	1.7 MB
☑	Communications	5.6 MB
□	Desktop Themes	0.0 MB
☑	Games	10.1 MB
□	Multilanguage Support	0.0 MB

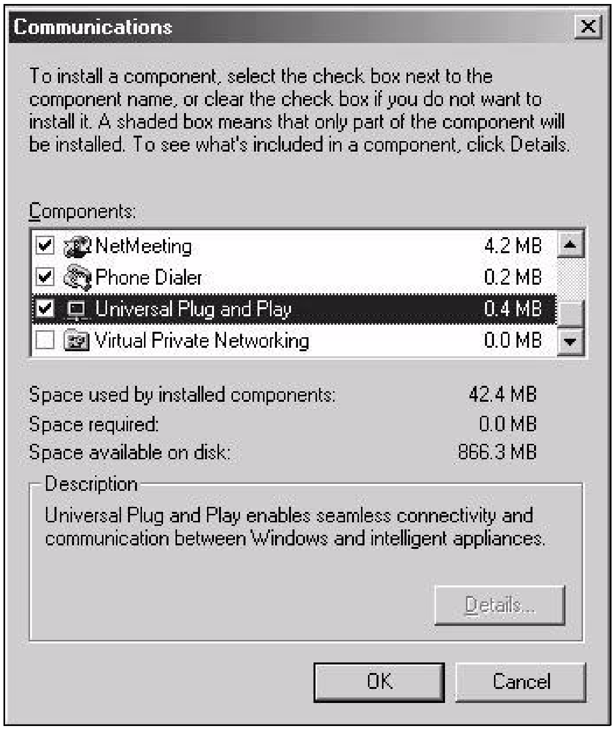
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

Description

Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.



To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	NetMeeting	4.2 MB
☑	Phone Dialer	0.2 MB
☑	Universal Plug and Play	0.4 MB
□	Virtual Private Networking	0.0 MB

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

Description

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

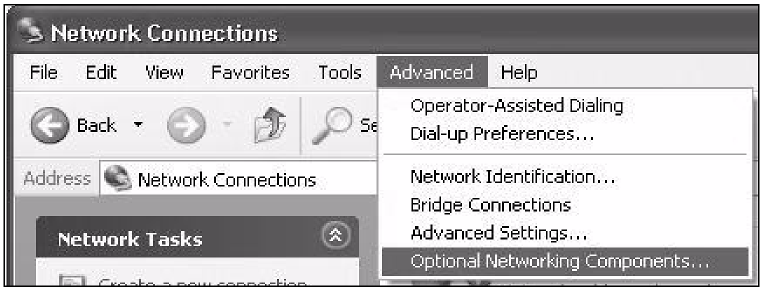
Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

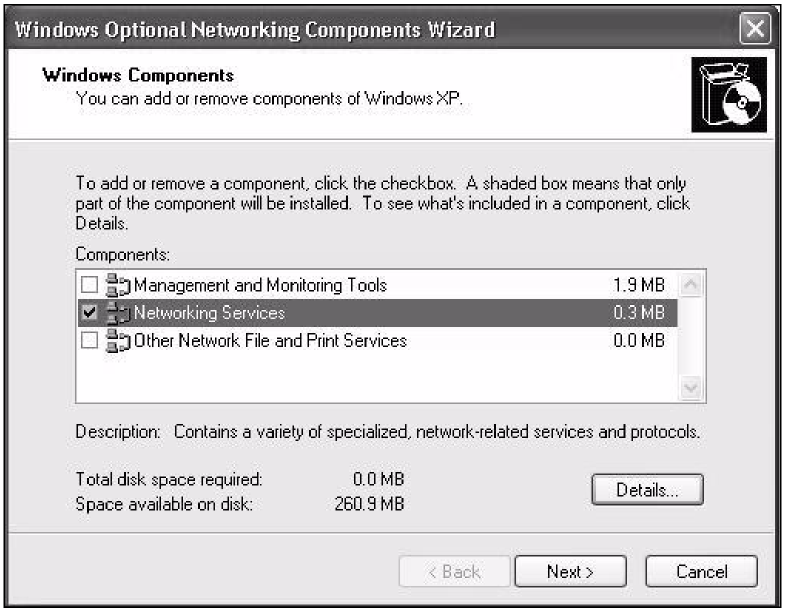
1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.



4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.



Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

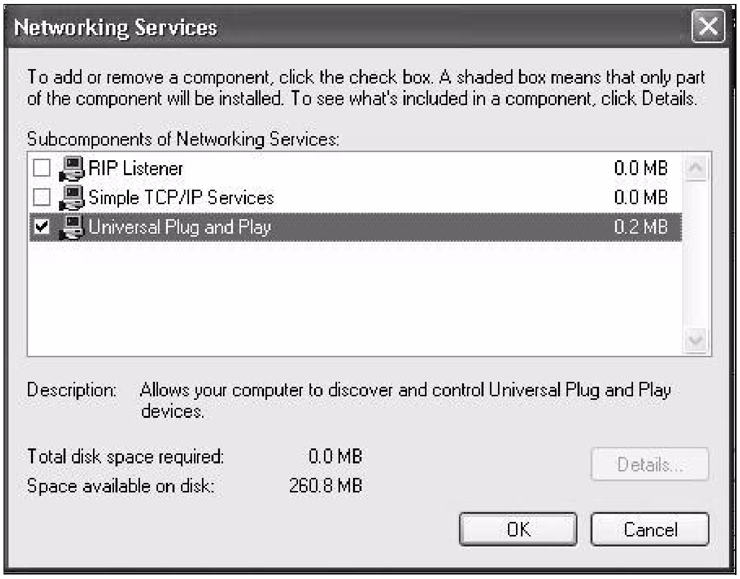
□	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 260.9 MB

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□ RIP Listener	0.0 MB
□ Simple TCP/IP Services	0.0 MB
☑ Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB

Space available on disk: 260.8 MB

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

7.6 Using UPnP in Windows XP Example

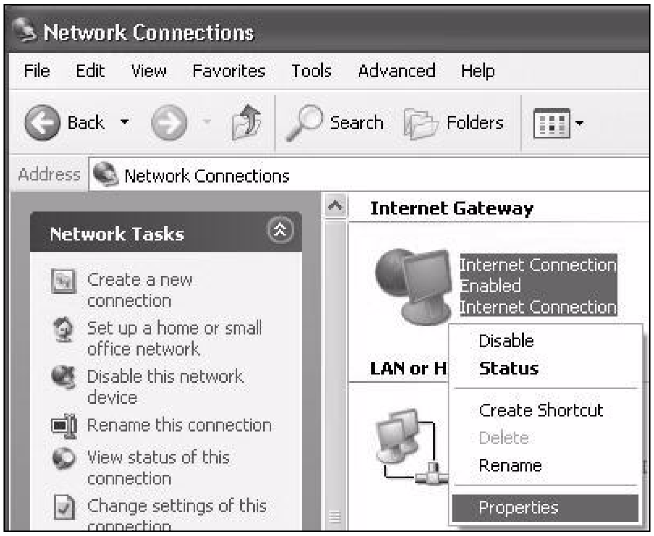
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL Device.

Make sure the computer is connected to a LAN port of the ZyXEL Device. Turn on your computer and the ZyXEL Device.

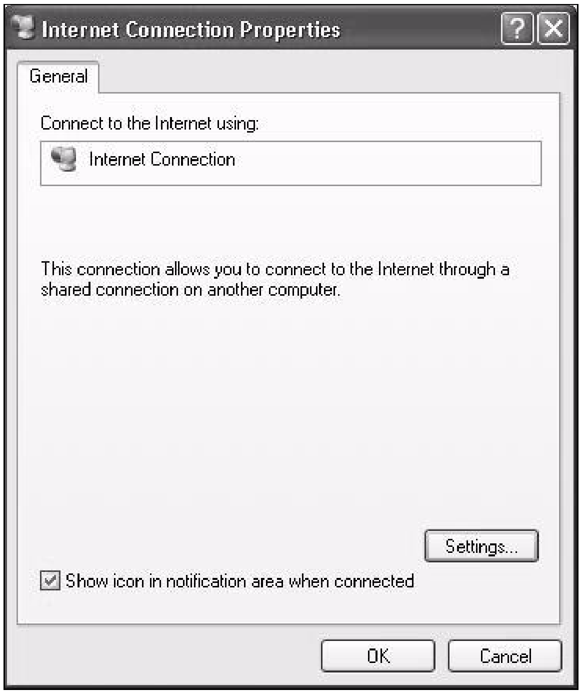
Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

2 Right-click the icon and select **Properties**.



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.



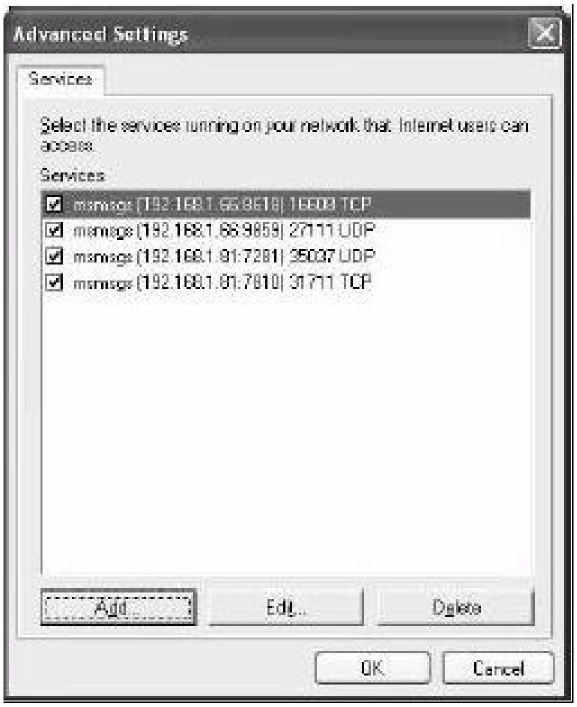
Connect to the Internet using:

Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.



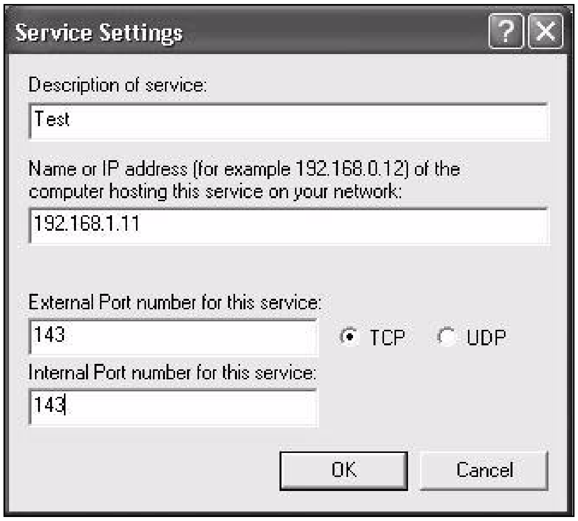
Advanced Settings

Services

Select the services running on your network that Internet users can access.

Services

☑ msmsgs (192.168.1.66:8618) 16608 TCP
☑ msmsgs (192.168.1.66:9859) 27111 UDP
☑ msmsgs (192.168.1.81:7281) 35037 UDP
☑ msmsgs (192.168.1.81:7810) 31711 TCP



Service Settings

Description of service:
Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
192.168.1.11

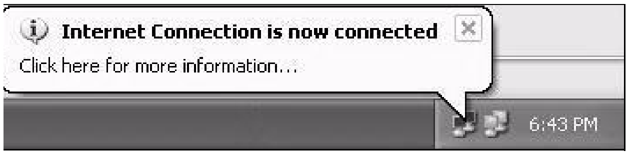
External Port number for this service:
143

● TCP ○ UDP

Internal Port number for this service:
143

5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

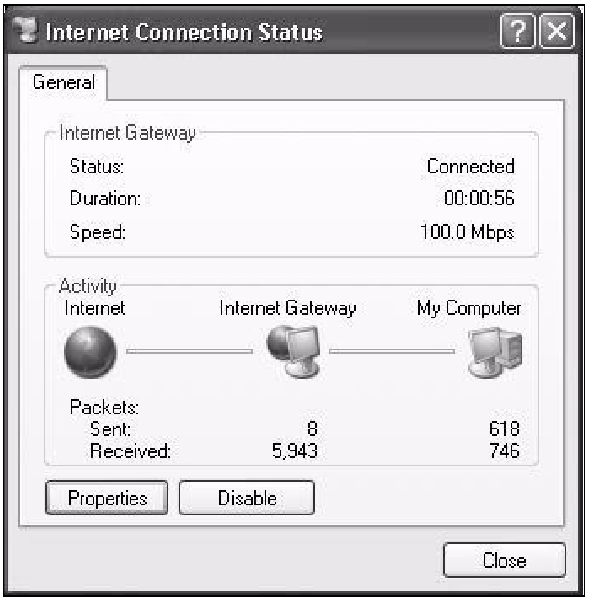
6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.



Internet Connection is now connected

Click here for more information...

7 Double-click on the icon to display your current Internet connection status.



Status:		Connected
Duration:		00:00:56
Speed:		100.0 Mbps
Packets:		
Sent:	8	618
Received:	5,943	746

Web Configurator Easy Access

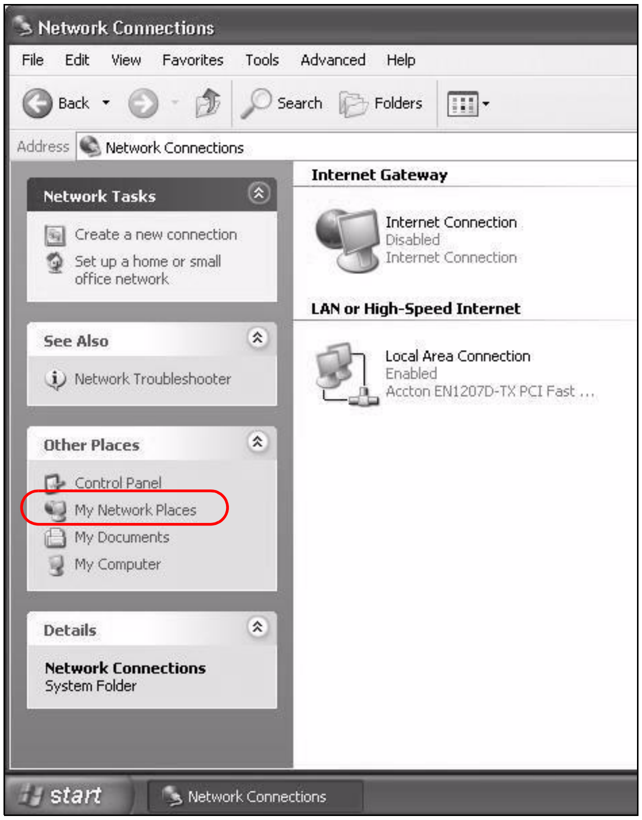
With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

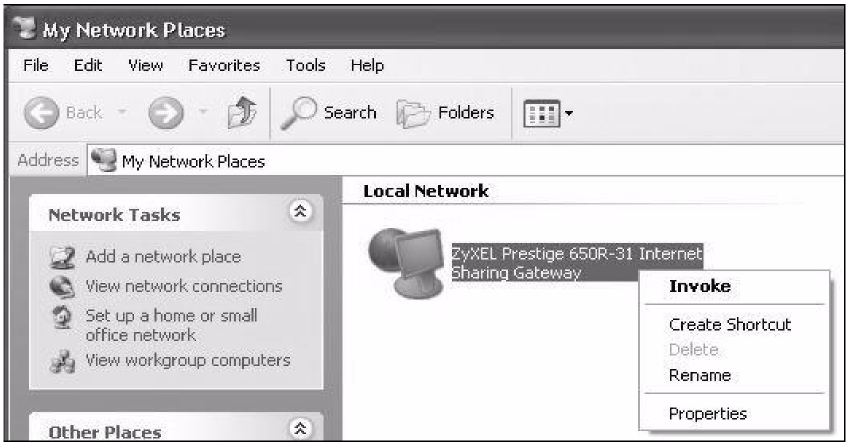
2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

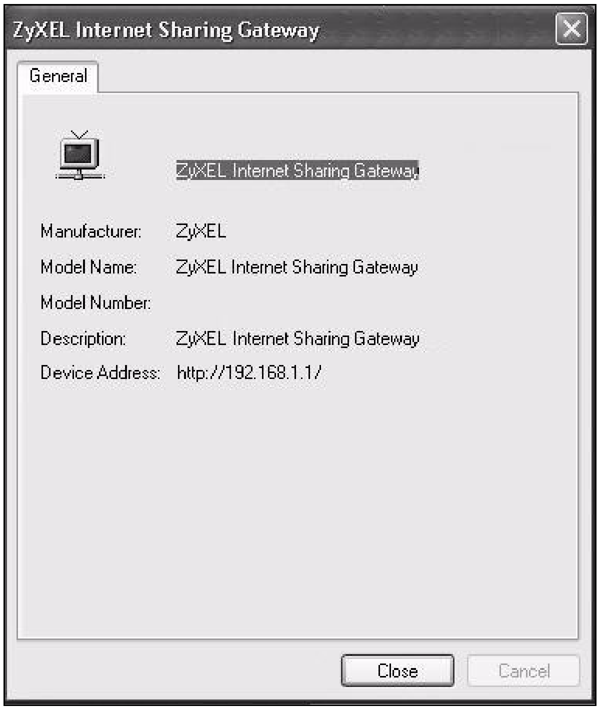


4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.



6 Right-click on the icon for your ZyXEL Device and select **Properties**. A properties window displays with basic information about the ZyXEL Device.



ZyXEL Internet Sharing Gateway
General
ZyXEL Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number:

Description: ZyXEL Internet Sharing Gateway

Device Address: http://192.168.1.1/

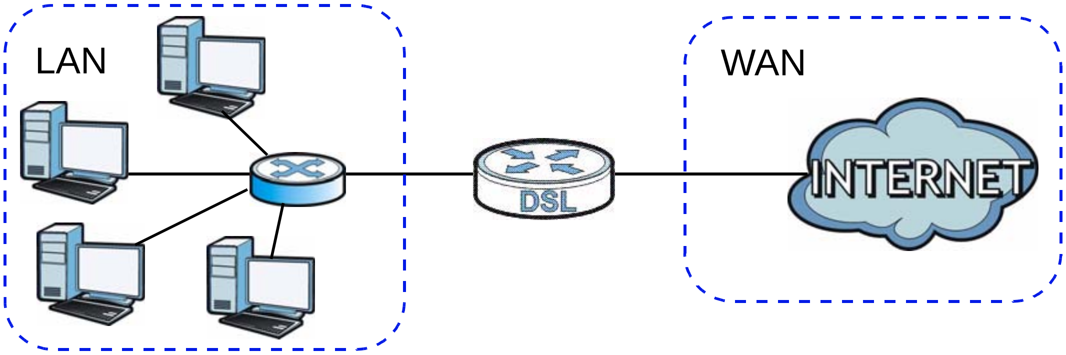
7.7 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

7.7.1 LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the ZyXEL Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 41 LAN and WAN IP Addresses



7.7.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

7.7.3 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **DHCP Setup** screen.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ZyXEL Device supports the IPCP DNS server extensions through the DNS proxy feature.

  Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen.

7.7.4 LAN TCP/IP

The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyXEL Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

8

Network Address Translation (NAT)

8.1 Overview

This chapter discusses how to configure NAT on the ZyXEL Device. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

8.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network (Section 8.2 on page 134).
- Use the **Applications** screen to forward incoming service requests to the server(s) on your local network (Section 8.3 on page 137).
- Use the **Port Triggering** screen to add and configure the ZyXEL Device's trigger port settings (Section 8.4 on page 139).
- Use the **DMZ** screen to configure a default server (Section 8.5 on page 143).
- Use the **ALG** screen to enable and disable the SIP (VoIP) ALG in the ZyXEL Device (Section 8.6 on page 144).
- Use the **Sessions** screen to limit the number of concurrent NAT sessions all clients can use (Section 8.7 on page 144).

8.1.2 What You Need To Know

Inside/Outside

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See Section 8.8 on page 145 for advanced technical information on NAT.

8.2 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

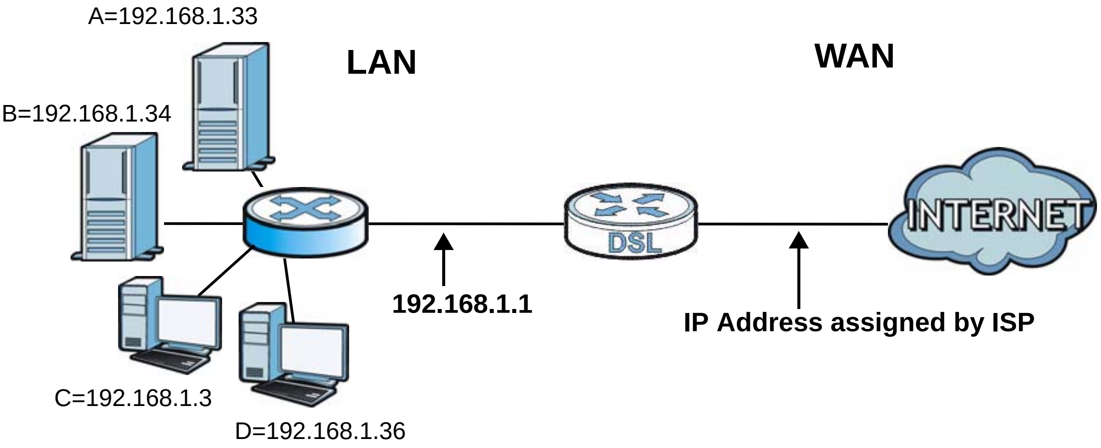
The most often used port numbers and services are shown in Appendix E on page 347. Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

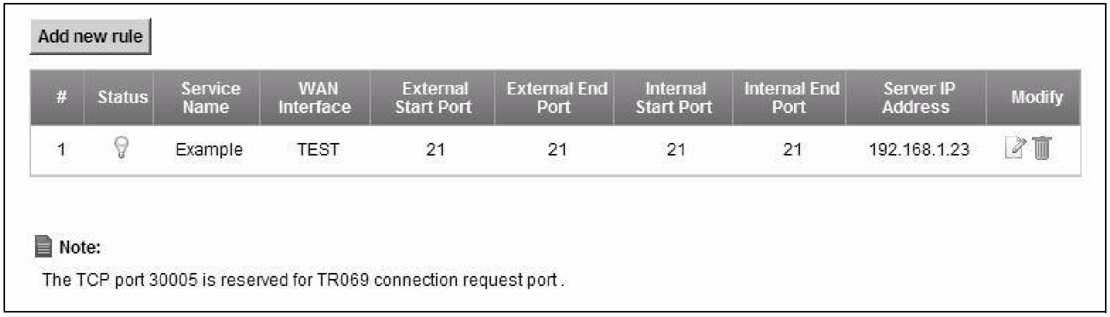
Figure 42 Multiple Servers Behind NAT Example



Click **Network Settings > NAT > Port Forwarding** to open the following screen.

See Appendix E on page 347 for port numbers commonly used for particular services.

Figure 43 Network Settings > NAT > Port Forwarding



#	Status	Service Name	WAN Interface	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Modify
1	💡	Example	TEST	21	21	21	21	192.168.1.23	✎ 🗑

Note:

The TCP port 30005 is reserved for TR069 connection request port .

The following table describes the fields in this screen.

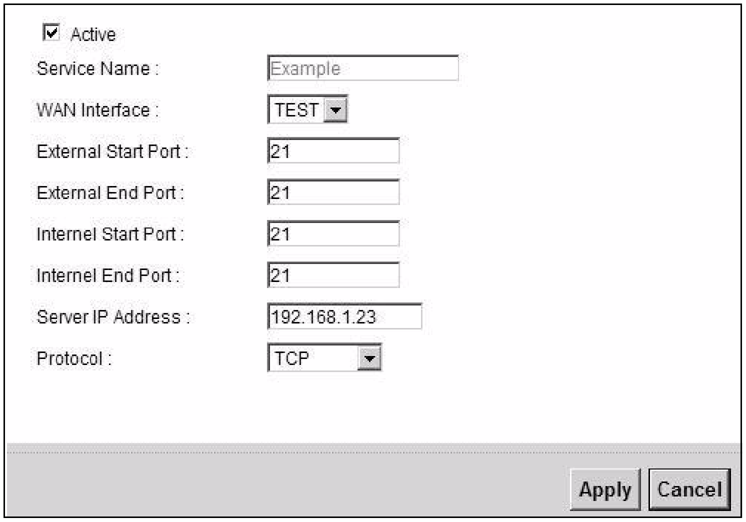
Table 27 Network Settings > NAT > Port Forwarding

LABEL	DESCRIPTION
Add new rule	Click this to add a new rule.
#	This is the index number of the entry.
Status	This field displays whether the NAT rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This shows the service’s name.
WAN Interface	This shows the WAN interface through which the service is forwarded.
External Start Port	This is the first external port number that identifies a service.
External End Port	This is the last external port number that identifies a service.
Internal Start Port	This is the first internal port number that identifies a service.
Internal End Port	This is the last internal port number that identifies a service.
Server IP Address	This is the server’s IP address.
Modify	Click the **Edit** icon to edit this rule. Click the **Delete** icon to delete an existing rule.

8.2.1 Add/Edit Port Forwarding

Click **Add new rule** in the **Port Forwarding** screen or click the **Edit** icon next to an existing rule to open the following screen.

Figure 44 Port Forwarding: Add/Edit



☑ Active

Service Name :	Example
WAN Interface :	TEST
External Start Port :	21
External End Port :	21
Internel Start Port :	21
Internel End Port :	21
Server IP Address :	192.168.1.23
Protocol :	TCP

The following table describes the labels in this screen.

Table 28 Port Forwarding: Add/Edit

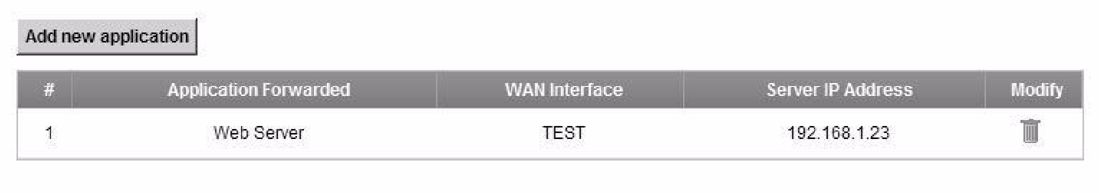
LABEL	DESCRIPTION
Active	Clear the check box to disable the rule. Select the check box to enable it. This field is read-only in the **Port Forwarding Configuration** screen.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on). This field is read-only in the **Port Forwarding Edit** screen.
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
External Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **External End Port** field.
External End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Start Port** field above.
Internal Start Port	This shows the port number to which you want the ZyXEL Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Internal End Port	This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol Type	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

8.3 The Applications Screen

This screen provides a summary of all NAT applications and their configuration. In addition, this screen allows you to create new applications and/or remove existing ones.

To access this screen, click **Network Settings > NAT > Applications**. The following screen appears.

Figure 45 Network Settings > NAT > Applications



#	Application Forwarded	WAN Interface	Server IP Address	Modify
1	Web Server	TEST	192.168.1.23	🗑

The following table describes the labels in this screen.

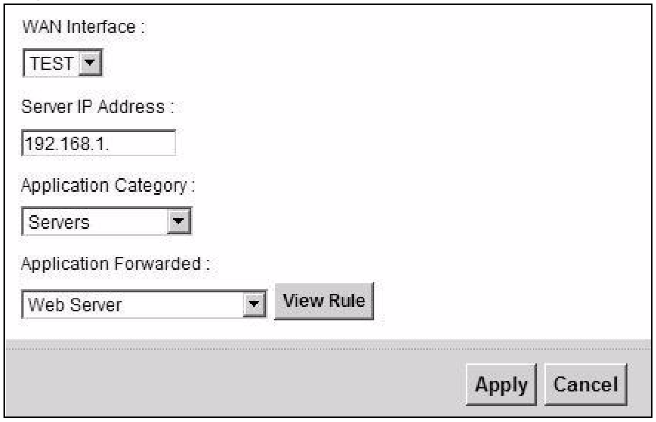
Table 29 Network Settings > NAT > Applications

LABEL	DESCRIPTION
Add new application	Click this to add a new NAT application rule.
Application Forwarded	This field shows the type of application that the service forwards.
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Server IP Address	This field displays the destination IP address for the service.
Modify	Click the **Delete** icon to delete the rule.

8.3.1 Add New Application

This screen lets you create new NAT application rules. Click **Add new application** in the **Applications** screen to open the following screen.

Figure 46 Applications: Add



WAN Interface : TEST

Server IP Address : 192.168.1.

Application Category : Servers

Application Forwarded : Web Server

The following table describes the labels in this screen.

Table 30 Applications: Add

LABEL	DESCRIPTION
WAN Interface	Select the WAN interface that you want to apply this NAT rule to.
Server IP Address	Enter the inside IP address of the application here.
Application Category	Select the category of the application from the drop-down list box.
Application Forwarded	Select a service from the drop-down list box and the ZyXEL Device automatically configures the protocol, start, end, and map port number that define the service.
View Rule	Click this to display the configuration of the service that you have chosen in **Application Fowarded**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

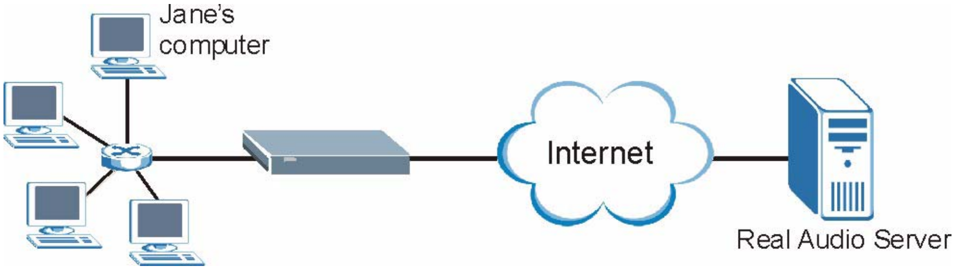
8.4 The Port Triggering Screen

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyXEL Device records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyXEL Device's WAN port receives a response with a specific port number and protocol ("open" port), the ZyXEL Device forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

Figure 47 Trigger Port Forwarding Process: Example



1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a “trigger” port and causes the ZyXEL Device to record Jane’s computer IP address. The ZyXEL Device associates Jane's computer IP address with the "open" port range of 6970-7170.

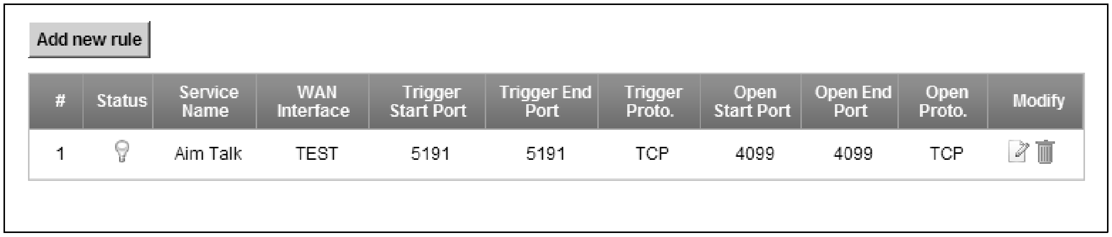
3 The Real Audio server responds using a port number ranging between 6970-7170.

4 The ZyXEL Device forwards the traffic to Jane’s computer IP address.

5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyXEL Device times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Network Settings > NAT > Port Triggering** to open the following screen. Use this screen to view your ZyXEL Device’s trigger port settings.

Figure 48 Network Settings > NAT > Port Triggering



#	Status	Service Name	WAN Interface	Trigger Start Port	Trigger End Port	Trigger Proto.	Open Start Port	Open End Port	Open Proto.	Modify
1	💡	Aim Talk	TEST	5191	5191	TCP	4099	4099	TCP	✎ 🗑

The following table describes the labels in this screen.

Table 31 Network Settings > NAT > Port Triggering

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This field displays the name of the service used by this rule.

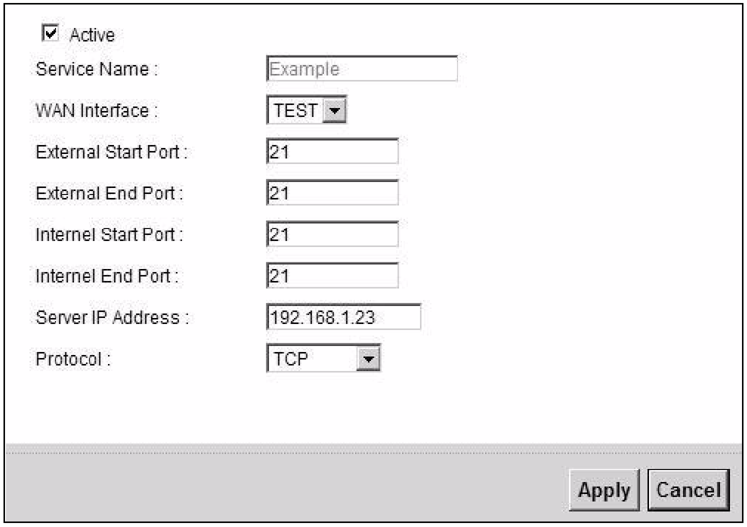
Table 31 Network Settings > NAT > Port Triggering (continued)

LABEL	DESCRIPTION
WAN Interface	This field shows the WAN interface through which the service is forwarded.
Trigger Port	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start	This is the first port number that identifies a service.
End	This is the last port number that identifies a service.
Trigger Proto.	This is the trigger transport layer protocol.
Open	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start	This is the first port number that identifies a service.
End	This is the last port number that identifies a service.
Open Proto.	This is the open transport layer protocol.
Modify	Click the **Edit** icon to edit this rule. Click the **Delete** icon to delete an existing rule.

8.4.1 Add/Edit Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add new rule** in the **Port Triggering** screen or click a rule's **Edit** icon to open the following screen.

Figure 49 Port Triggering: Add/Edit



☑ Active

Service Name : Example

WAN Interface : TEST

External Start Port : 21

External End Port : 21

Internel Start Port : 21

Internel End Port : 21

Server IP Address : 192.168.1.23

Protocol : TCP

The following table describes the labels in this screen.

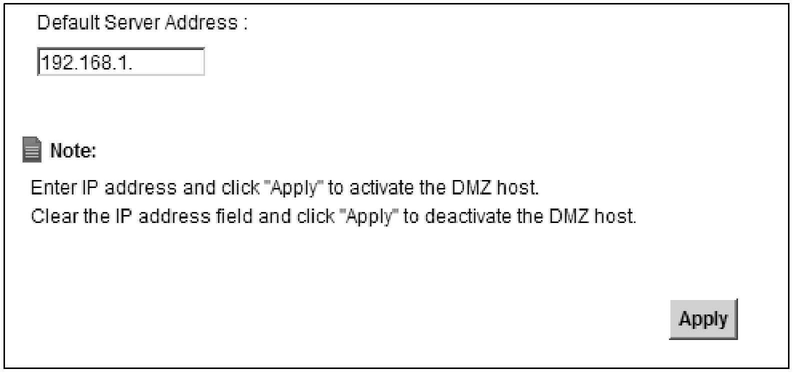
Table 32 Port Triggering: Configuration Add/Edit

LABEL	DESCRIPTION
Active	Select the check box to enable this rule. This field is read-only in the **Port Triggering Configuration** screen.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on). This field is read-only in the **Port Triggering Edit** screen.
WAN Interface	Select a WAN interface for which you want to configure port triggering rules.
Trigger Start Port	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyXEL Device to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
Trigger End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Open Start Port	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyXEL Device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open End Port	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

8.5 The DMZ Screen

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in the **NAT Port Forwarding Setup** screen.

Figure 50 Network Settings > NAT > DMZ



Default Server Address :

192.168.1.

Note:

Enter IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to deactivate the DMZ host.

The following table describes the fields in this screen.

Table 33 Network Settings > NAT > DMZ

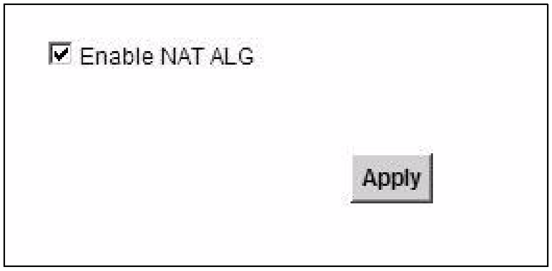
LABEL	DESCRIPTION
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the **NAT Port Forwarding** screen. Note: If you do not assign a **Default Server Address**, the ZyXEL Device discards all packets received for ports that are not specified in the **NAT Port Forwarding** screen.
Apply	Click **Apply** to save your changes.

8.6 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the ZyXEL Device registers with the SIP register server, the SIP ALG translates the ZyXEL Device’s private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your ZyXEL Device is behind a SIP ALG.

Use this screen to enable and disable the SIP (VoIP) ALG in the ZyXEL Device. To access this screen, click **Network Settings > NAT > ALG**.

Figure 51 Network Settings > NAT > ALG



☑ Enable NAT ALG

The following table describes the fields in this screen.

Table 34 Network Settings > NAT > ALG

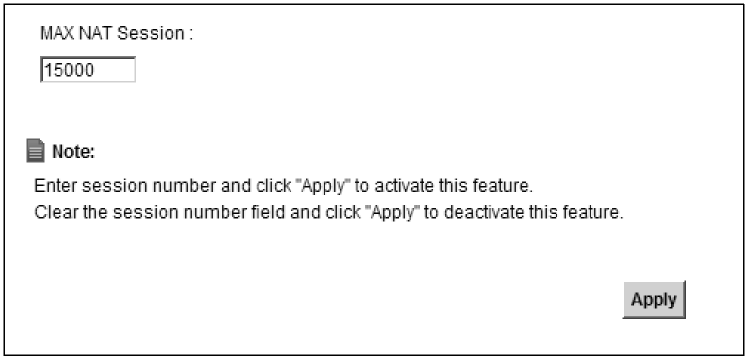
LABEL	DESCRIPTION
Enable SIP ALG	Select this to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
Apply	Click **Apply** to save your changes.

8.7 The Sessions Screen

Use the **Sessions** screen to limit the number of concurrent NAT sessions all clients can use.

Click **Network Settings > NAT > Sessions** to display the following screen.

Figure 52 Network Settings > NAT > Sessions



MAX NAT Session :

15000

Note:

Enter session number and click "Apply" to activate this feature.
Clear the session number field and click "Apply" to deactivate this feature.

The following table describes the fields in this screen.

Table 35 Network Settings > NAT > Sessions

LABEL	DESCRIPTION
MAX NAT Session	Use this field to set a common limit to the number of concurrent NAT sessions all client computers can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Apply	Click **Apply** to save your changes.

8.8 Technical Reference

This part contains more information regarding NAT.

8.8.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 36 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

8.8.2 What NAT Does

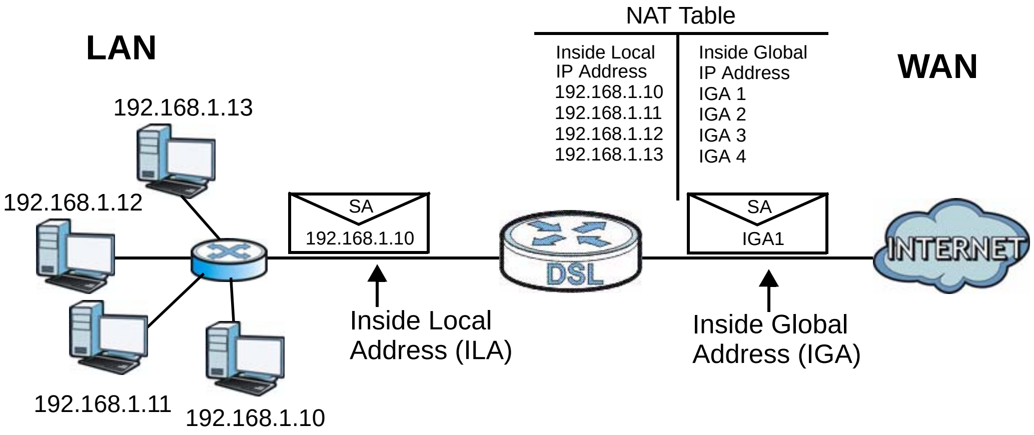
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

8.8.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyXEL Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 53 How NAT Works



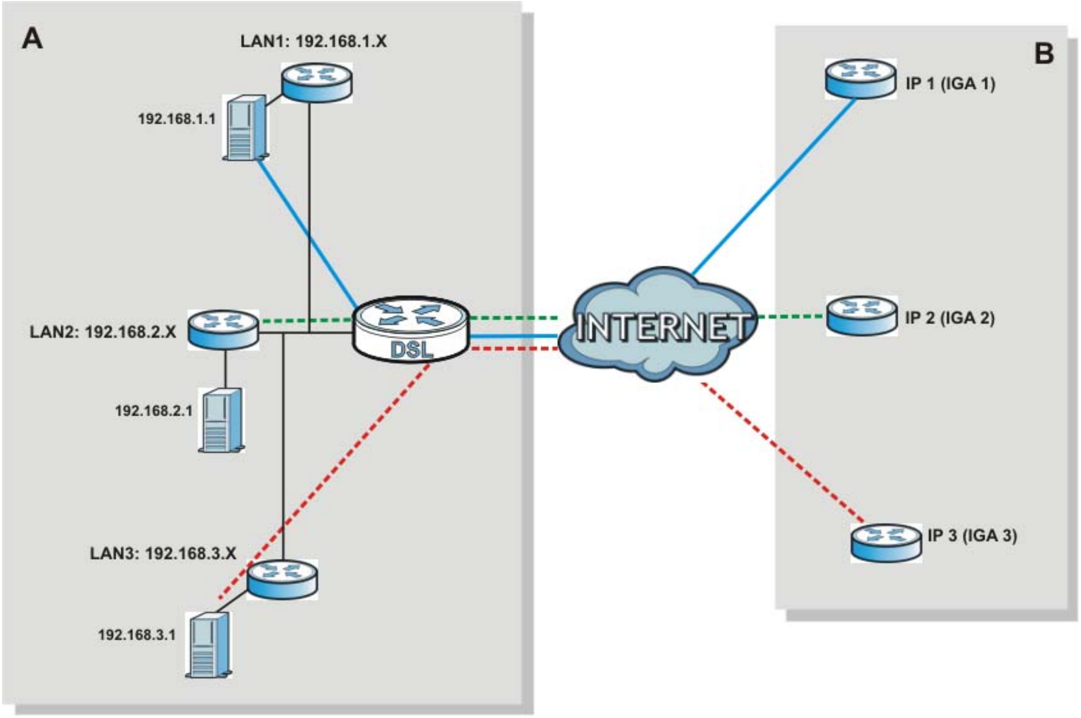
NAT Table

Inside Local IP Address	Inside Global IP Address
192.168.1.10	IGA 1
192.168.1.11	IGA 2
192.168.1.12	IGA 3
192.168.1.13	IGA 4

8.8.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the ZyXEL Device can communicate with three distinct WAN networks.

Figure 54 NAT Application With IP Alias



Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

Table 37 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161

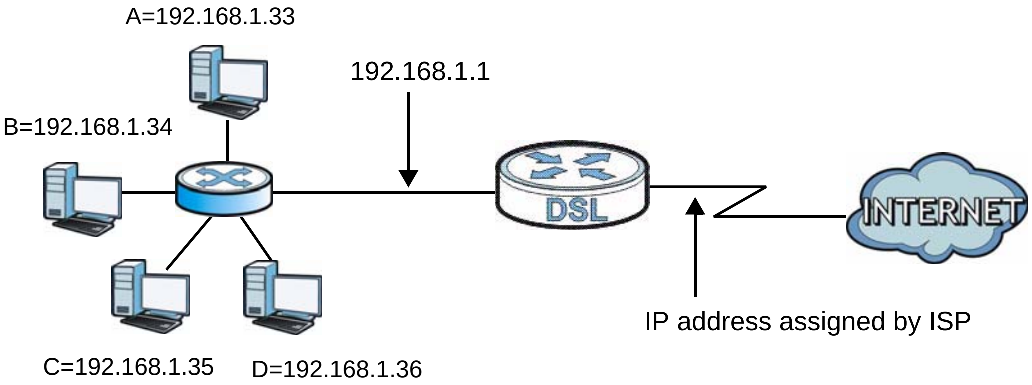
Table 37 Services and Port Numbers (continued)

SERVICES	PORT NUMBER
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 55 Multiple Servers Behind NAT Example



MAC Filter

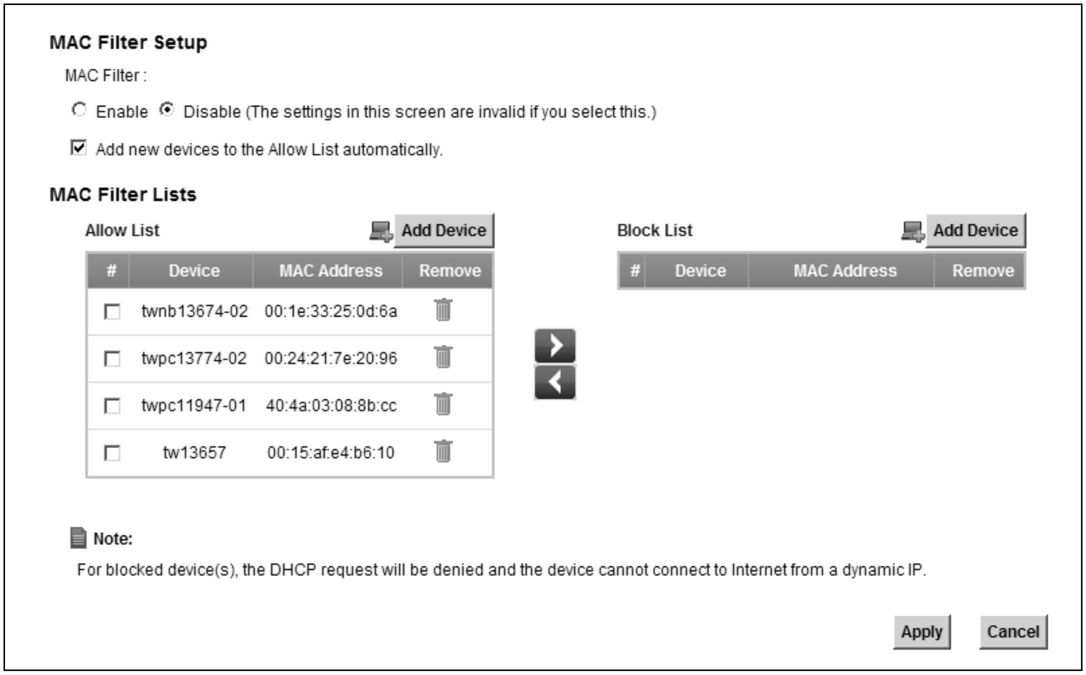
9.1 Overview

This screen allows you to configure the ZyXEL Device to give exclusive access to specific devices or exclude specific devices from accessing the ZyXEL Device. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

9.2 The MAC Filter Screen

Use this screen to change your ZyXEL Device's MAC filter settings. Click **Security Settings** > **MAC Filter**. The screen appears as shown.

Figure 56 Security Settings > MAC Filter



MAC Filter Setup

MAC Filter :

○ Enable ● Disable (The settings in this screen are invalid if you select this.)

☑ Add new devices to the Allow List automatically.

MAC Filter Lists

Allow List

#	Device	MAC Address	Remove
□	twnb13674-02	00:1e:33:25:0d:6a	🗑
□	twpc13774-02	00:24:21:7e:20:96	🗑
□	twpc11947-01	40:4a:03:08:8b:cc	🗑
□	tw13657	00:15:af:e4:b6:10	🗑

Block List

#	Device	MAC Address	Remove

Note:

For blocked device(s), the DHCP request will be denied and the device cannot connect to Internet from a dynamic IP.

The following table describes the labels in this screen.

Table 38 Security Settings > MAC Filter

LABEL	DESCRIPTION
MAC Filter Setup	
MAC Filter	Select **Enable** to activate the MAC filter function. Otherwise, select **Disable**.
Add new devices to the Allow List automatically	Select this check box if you want the ZyXEL Device to automatically add the newly connected devices to the **Allow List**.
MAC Filter Lists	
Allow List Block List	The devices in this list are permitted or denied access to the ZyXEL Device. Select an entry from the **Allow List** and use the **>** button to add it to the **Block List**. Select an entry from the **Block List** and use the **<** button to add it to the **Allow List**.
Add Device	Select this to display the **Add Device** screen which you can add a device to the MAC filter **Allow List**. Enter the device's MAC address and click **OK**.
#	This is the index number of the entry.
Device	This is the name of the device that is allowed access to the ZyXEL Device.
MAC Address	This is the MAC address of the device that is allowed access to the ZyXEL Device.
Remove	Select the entry(ies) that you want to delete in the **Remove** column, then click the **Delete** icon.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10

Firewall

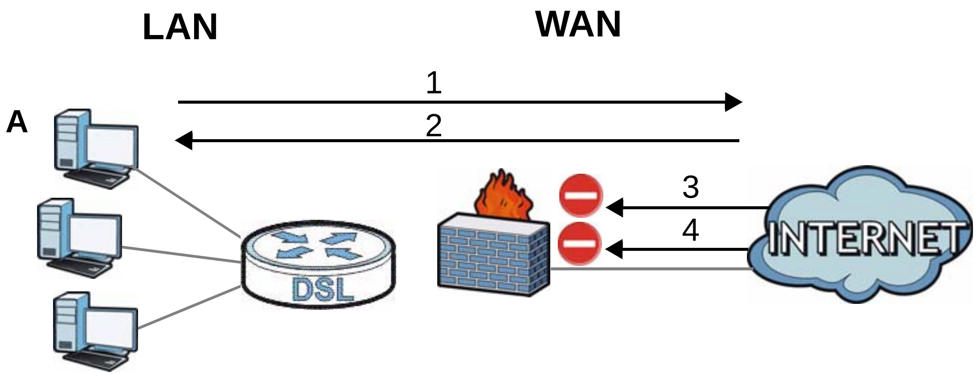
10.1 Overview

This chapter shows you how to enable and configure the ZyXEL Device firewall. Use the firewall to protect your ZyXEL Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 57 Default Firewall Action



10.1.1 What You Can Do in this Chapter

- Use the **Firewall** screen to configure the security level of the firewall on the ZyXEL Device (Section 10.2 on page 155).
- Use the **Protocol** screen to add or remove predefined Internet services and configure firewall rules (Section 10.3 on page 155).
- Use the **Access Control** screen to view and configure incoming/outgoing filtering rules (Section 10.4 on page 157).

10.1.2 What You Need to Know

SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

DDoS

A DDoS attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

SPI

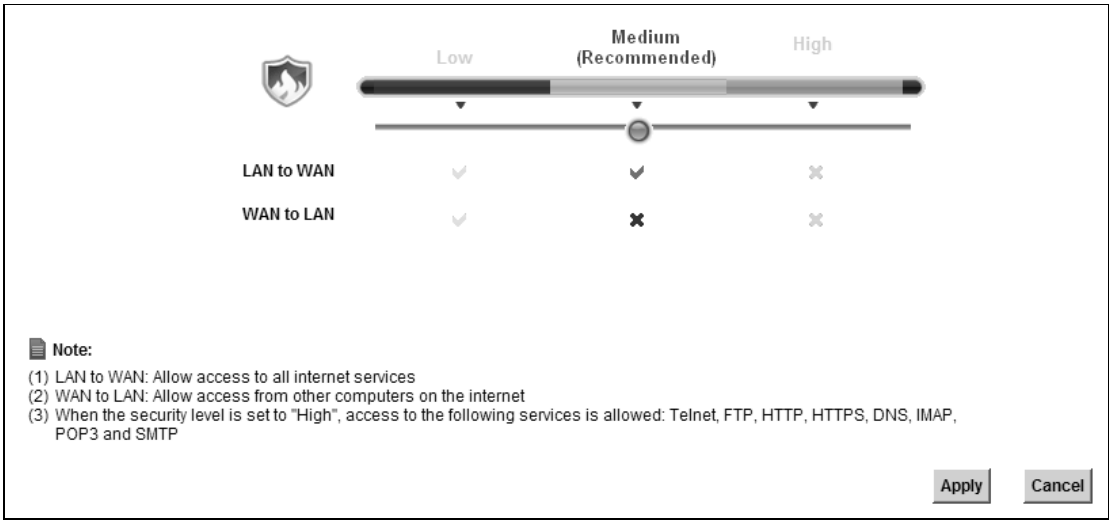
Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

10.2 The Firewall Screen

Use this screen to set the security level of the firewall on the ZyXEL Device. Firewall rules are grouped based on the direction of travel of packets to which they apply.

Click **Security Settings > Firewall** to display the following screen. Select a direction of travel of packets for which you want to configure firewall rules.

Figure 58 Security Settings > Firewall



	Low	Medium (Recommended)	High
LAN to WAN	✓	✓	✗
WAN to LAN	✓	✗	✗

Note:
(1) LAN to WAN: Allow access to all internet services
(2) WAN to LAN: Allow access from other computers on the internet
(3) When the security level is set to "High", access to the following services is allowed: Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP

The following table describes the labels in this screen.

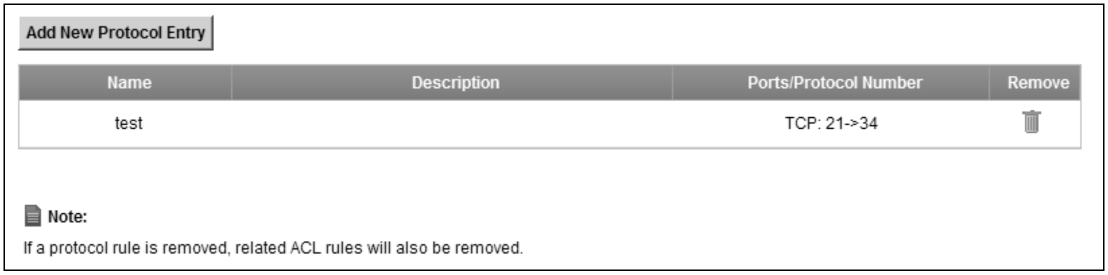
Table 39 Security Settings > Firewall

LABEL	DESCRIPTION
Low	Select **Low** to allow LAN to WAN and WAN to LAN packet directions.
Medium	Select **Medium** to allow LAN to WAN but deny WAN to LAN packet directions.
High	Select **High** to deny LAN to WAN and WAN to LAN packet directions.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.3 The Protocol Screen

You can configure customized services and port numbers in the **Protocol** screen. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. See Appendix E on page 347 for some examples.

Click **Security Settings > Protocol** to display the following screen.



Name	Description	Ports/Protocol Number	Remove
test		TCP: 21->34	🗑

Note:

If a protocol rule is removed, related ACL rules will also be removed.

Figure 59 Security Settings > Protocol

The following table describes the labels in this screen.

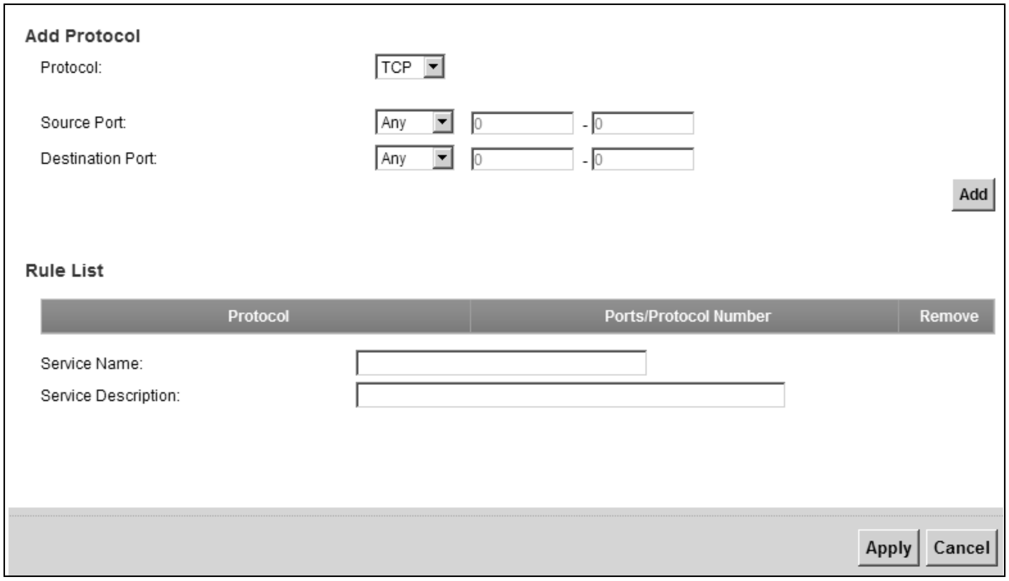
Table 40 Security Settings > Protocol

LABEL	DESCRIPTION
Add New Protocol Entry	Click this to add a new protocol.
Name	This is the name of your customized service.
Description	This is the description of your customized service.
Ports/ Protocol Number	This shows the port number or range and IP protocol (**TCP**, **UDP** or **TCP/ UDP**) that defines your customized service
Remove	Click the **Delete** icon to remove this entry.

10.3.1 Add a Protocol

Use this screen to add a customized rule. Click **Add New Protocol Entry** in the **Protocol** screen to display the following screen.

Figure 60 Protocol: Add



Add Protocol

Protocol:	TCP		
Source Port:	Any	0	- 0
Destination Port:	Any	0	- 0

Rule List

Protocol	Ports/Protocol Number	Remove

Service Name:

Service Description:

The following table describes the labels in this screen.

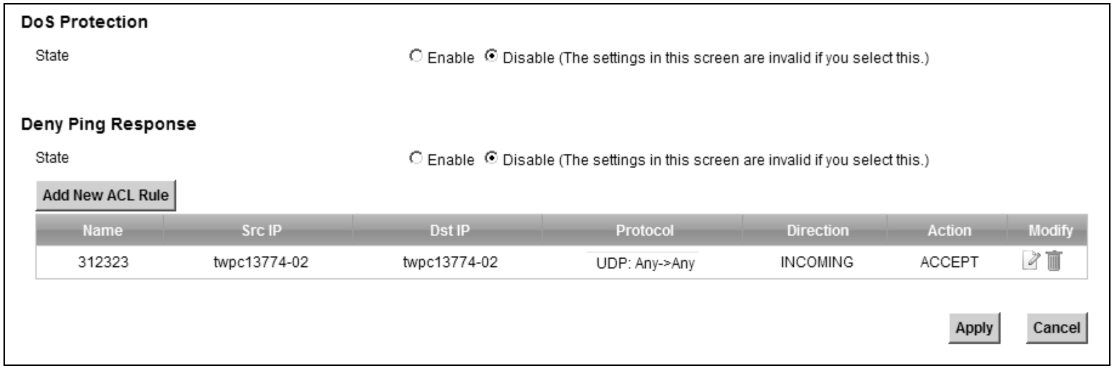
Table 41 Protocol: Add

LABEL	DESCRIPTION
Add Protocol	
Protocol	Choose the IP port (**TCP**, **UDP**, **ICMP**, or **Other**) that defines your customized port from the drop-down list box. Select **Other** to apply the rule to any protocol.
Source/ Destination Port	These fields are displayed if you select **TCP** or **UDP** as the IP port. Select **Single** to specify one port only or **Range** to specify a span of ports that define your customized service. If you select **Any**, the service is applied to all ports. Type a single port number or the range of port numbers that define your customized service.
Protocol Number	This field is displayed if you select **Other** as the IP port. Enter the number of your customized port.
Add	Click this to add the protocol to the **Rule List** below.
Rule List	
Service Name	Enter a unique name (up to 32 printable English keyboard characters, including spaces) for your customized port.
Service Description	Enter a description for your customized port.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

10.4 The Access Control Screen

Click **Security Settings > Access Control** to display the following screen. This screen displays a list of the configured incoming or outgoing filtering rules.

Figure 61 Security Settings > Access Control



DoS Protection

State ○ Enable ● Disable (The settings in this screen are invalid if you select this.)

Deny Ping Response

State ○ Enable ● Disable (The settings in this screen are invalid if you select this.)

Name	Src IP	Dst IP	Protocol	Direction	Action	Modify
312323	twpc13774-02	twpc13774-02	UDP: Any->Any	INCOMING	ACCEPT	

The following table describes the labels in this screen.

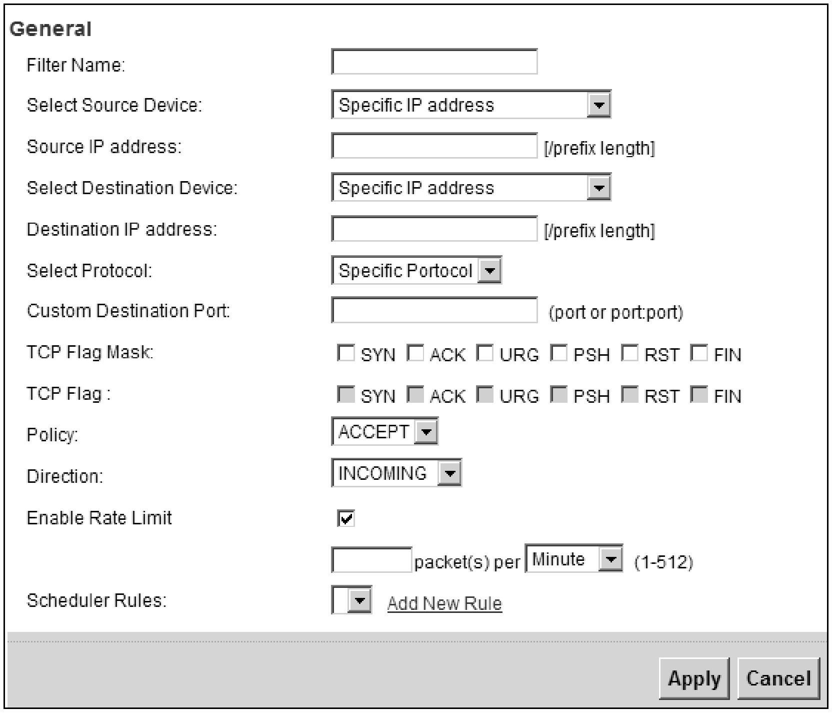
Table 42 Security Settings > Access Control

LABEL	DESCRIPTION
DoS Protection	DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. Select the **Enable** check box to enable protection against DoS attacks.
Deny Ping Response	Select the **Enable** check box to block ping packets.
Add New ACL Rule	Click this to go to add a filter rule for incoming or outgoing IP traffic.
Name	This displays the name of the rule.
Srp IP	This displays the source IP addresses to which this rule applies. Please note that a blank source address is equivalent to **Any**.
Dst IP	This displays the destination IP addresses to which this rule applies. Please note that a blank destination address is equivalent to **Any**.
Protocol	This displays the transport layer protocol that defines the service to which this rule applies.
Direction	This displays the direction of traffic to which this rule applies.
Action	This field displays whether the rule silently discards packets (**DROP**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**REJECT**) or allows the passage of packets (**ACCEPT**).
Modify	Click the **Edit** icon to edit the rule. Click the **Delete** icon to delete an existing rule. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save the DoS Protection settings.
Cancel	Click **Cancel** to restore your previously saved settings.

10.4.1 Add/Edit an ACL Rule

Click **Add New ACL Rule** or the **Edit** icon next to an existing ACL rule in the **Access Control** screen. The following screen displays.

Figure 62 Access Control: Add/Edit



General	
Filter Name:	
Select Source Device:	Specific IP address
Source IP address:	[/prefix length]
Select Destination Device:	Specific IP address
Destination IP address:	[/prefix length]
Select Protocol:	Specific Portocol
Custom Destination Port:	(port or port:port)
TCP Flag Mask:	□ SYN □ ACK □ URG □ PSH □ RST □ FIN
TCP Flag :	□ SYN □ ACK □ URG □ PSH □ RST □ FIN
Policy:	ACCEPT
Direction:	INCOMING
Enable Rate Limit	☑
	packet(s) per Minute (1-512)
Scheduler Rules:	Add New Rule

The following table describes the labels in this screen.

Table 43 Access Control: Add/Edit

LABEL	DESCRIPTION
General	
Filter Name	Enter a descriptive name of up to 16 alphanumeric characters, not including spaces, underscores, and dashes. You must enter the filter name to add an ACL rule. This field is read-only if you are editing the ACL rule.
Select Source Device	Select the source device to which the ACL rule applies. If you select **Specific IP Address**, enter the source IP address in the field below.
Source IP Address	Enter the source IP address.
Select Destination Device	Select the destination device to which the ACL rule applies. If you select **Specific IP Address**, enter the destiniation IP address in the field below.
Destination IP Address	Enter the destination IP address.

Table 43 Access Control: Add/Edit (continued)

LABEL	DESCRIPTION
Select Protocol	Select the transport layer protocol that defines your customized port from the drop-down list box. If you want to configure a customized protocol, select **Specific Protocol**.
Protocol	This field is displayed only when you select **Specific Protocol** in **Select Protocol**. Choose the IP port (**TCP/UDP**, **TCP**, **UDP**, or **ICMP**) that defines your customized port from the drop-down list box.
Custom Source Port	This field is displayed only when you select **Specific Protocol** in **Select Protocol**. Enter a single port number or the range of port numbers of the source.
Custom Destination Port	This field is displayed only when you select **Specific Protocol** in **Select Protocol**. Enter a single port number or the range of port numbers of the destination.
TCP Flag Mask	This field is displayed only when you select **Specific Protocol** in **Select Protocol** and **TCP/UDP** or **TCP** as the protocol. You can select the TCP flags you want to check in this field. Select one or a combination of the following TCP flags: • **SYN:** synchronize flag • **ACK:** acknowledge flag • **URG:** urgent flag • **PSH:** push flag • **RST:** reset flag • **FIN:** finish flag
TCP Flag	This field is displayed only when you select **Specific Protocol** in **Select Protocol** and **TCP/UDP** or **TCP** as the protocol. After specifying the TCP flags to check, you can select the TCP flags you want to set. If a flag is set, the bit number is 1. If a flag is not set, the bit number is 0. The ZyXEL Device will take the action that you select in the **Policy** field below to the TCP flags that are set. You can only set the TCP flags that you have selected to check in the **TCP Flag Mask** field.
Policy	Use the drop-down list box to select whether to discard (**DROP**), deny and send an ICMP destination-unreachable message to the sender of (**REJECT**) or allow the passage of (**ACCEPT**) packets that match this rule.
Direction	Use the drop-down list box to select the direction of traffic to which this rule applies.
Enable Rate Limit	Select this check box to set a limit on the upstream/downstream transmission rate for the specified protocol. Specify how many packets per minute or second the transmission rate is.

Table 43 Access Control: Add/Edit (continued)

LABEL	DESCRIPTION
Scheduler Rules	Select a schedule rule for this ACL rule form the drop-down list box. You can configure a new schedule rule by click **Add new rule**. This will bring you to the **Advanced > Scheduler Rules** screen.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

11

Remote Management

11.1 Overview

This chapter provides information on the **Remote MGMT** screen.

Service Control allows you to manage your ZyXEL Device from a remote location through the following interfaces:

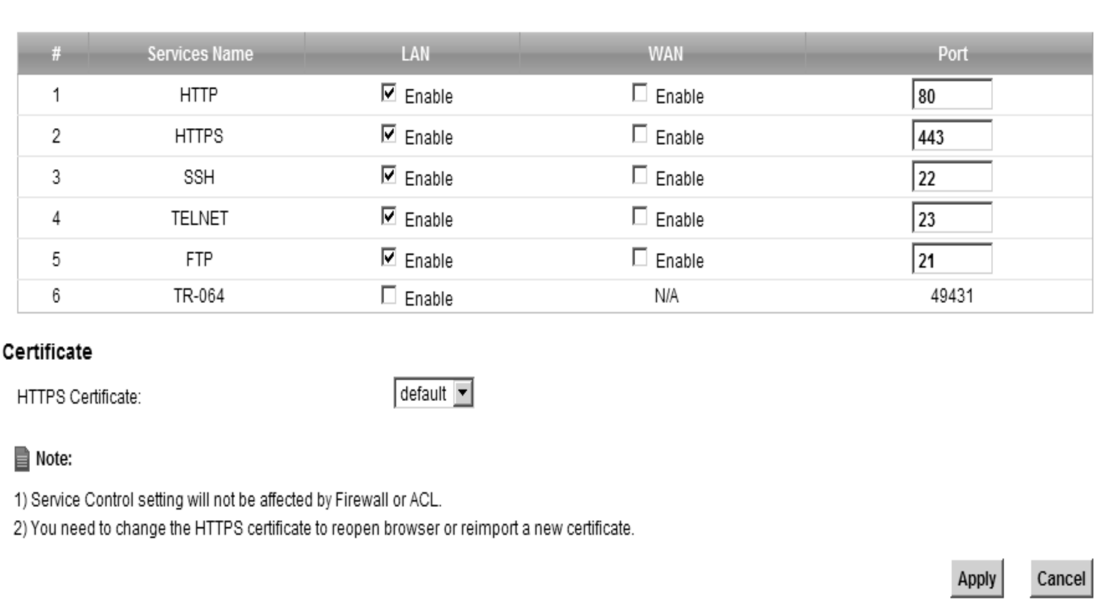
- LAN
- WAN

Note: The ZyXEL Device is managed using the Web Configurator.

11.2 The Service Control Screen

Use this screen to configure through which interface(s) users can use which service(s) to manage the ZyXEL Device.

Click **Security Settings > Service Control** to open the following screen.



#	Services Name	LAN	WAN	Port
1	HTTP	☑ Enable	□ Enable	80
2	HTTPS	☑ Enable	□ Enable	443
3	SSH	☑ Enable	□ Enable	22
4	TELNET	☑ Enable	□ Enable	23
5	FTP	☑ Enable	□ Enable	21
6	TR-064	□ Enable	N/A	49431

Certificate

HTTPS Certificate: default

Note:

1) Service Control setting will not be affected by Firewall or ACL.

2) You need to change the HTTPS certificate to reopen browser or reimport a new certificate.

Figure 63 Security Settings > Service Control

The following table describes the fields in this screen.

Table 44 Security Settings > Service Control

LABEL	DESCRIPTION
General	
#	This is the index number of the entry.
Services Name	This is the service you may use to access the ZyXEL Device.
LAN	Select the **Enable** check box for the corresponding services that you want to allow access to the ZyXEL Device from the LAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the ZyXEL Device from the WAN.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Certificate	
HTTPS Certificate	Select a certificate the HTTPS server (the ZyXEL Device) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **Certificates** screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to restore your previously saved settings.

12

Certificates

12.1 Overview

The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner’s identity and public key. Certificates provide a way to exchange public keys for use in authentication.

12.1.1 What You Can Do in this Chapter

- The **Local Certificates** screen lets you generate certification requests and import the ZyXEL Device's CA-signed certificates (Section 12.4 on page 172).
- The **Trusted CA** screen lets you save the certificates of trusted CAs to the ZyXEL Device (Section 12.4 on page 172).

12.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

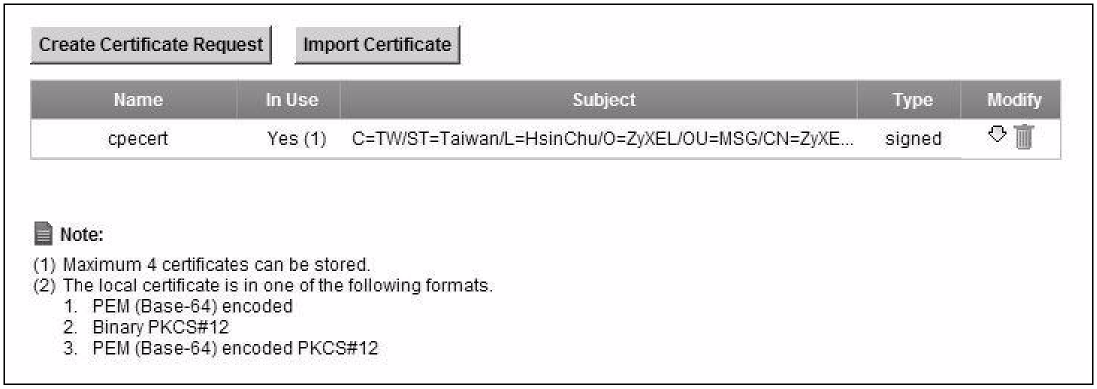
Certification Authority

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates. You can use the ZyXEL Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

12.3 The Local Certificates Screen

Click **Security Settings > Certificates** to open the **Local Certificates** screen. This is the ZyXEL Device's summary list of certificates and certification requests.

Figure 64 Security Settings > Certificates > Local Certificates



Name	In Use	Subject	Type	Modify
cpecert	Yes (1)	C=TW/ST=Taiwan/L=HsinChu/O=ZyXEL/OU=MSG/CN=ZyXE...	signed	

Note:
(1) Maximum 4 certificates can be stored.
(2) The local certificate is in one of the following formats.
1. PEM (Base-64) encoded
2. Binary PKCS#12
3. PEM (Base-64) encoded PKCS#12

The following table describes the labels in this screen.

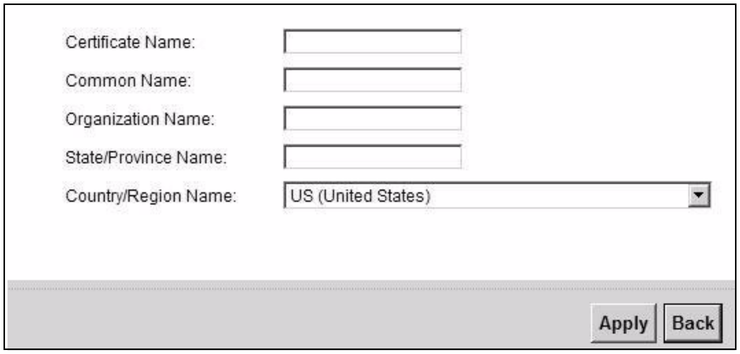
Table 45 Security Settings > Certificates > Local Certificates

LABEL	DESCRIPTION
Create Certificate Request	Click this button to go to the screen where you can have the ZyXEL Device generate a certification request.
Import Certificate	Click this button to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyXEL Device.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
In Use	This field displays how many applications use the certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Type	This field displays what kind of certificate this is. **request** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **Load Certificate** screen to import the certificate and replace the request. **signed** represents a certificate issued by a certification authority.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

12.3.1 Create Certificate Request

Click **Security Settings** > **Certificates** > **Local Certificates** and then **Create Certificate Request** to open the following screen. Use this screen to have the ZyXEL Device generate a certification request.

Figure 65 Create Certificate Request



Certificate Name:	
Common Name:	
Organization Name:	
State/Province Name:	
Country/Region Name:	US (United States)

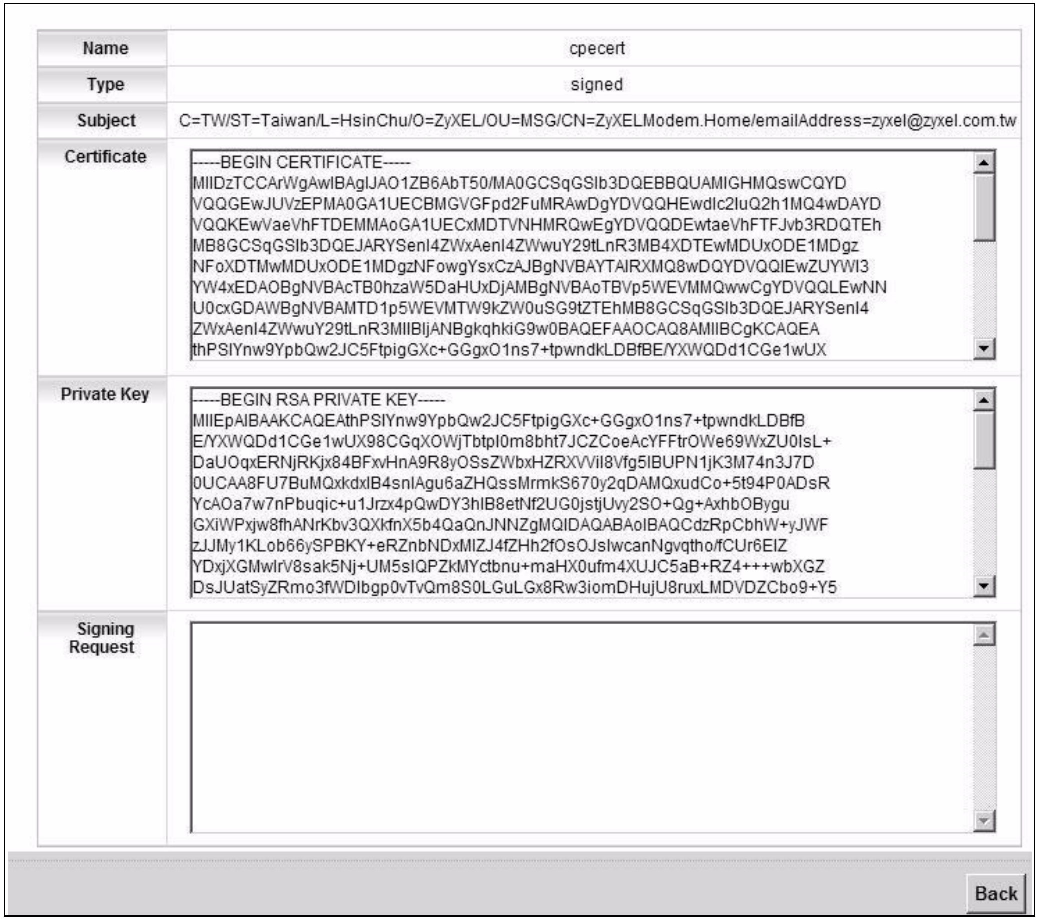
The following table describes the labels in this screen.

Table 46 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

After you click **Apply**, the **Certificate Request Details** screen displays. Click **Back** to return to the **Local Certificates** screen. See Section 12.3.3 on page 170 for field information.

Figure 66 Certificate Request Details



Name	cpecert
Type	signed
Subject	C=TW/ST=Taiwan/L=HsinChu/O=ZyXEL/OU=MSG/CN=ZyXELModem.Home/emailAddress=zyxel@zyxel.com.tw

Certificate

```
-----BEGIN CERTIFICATE-----
MIIDzTCCArWgAwIBAgIJAO1ZB6AbT50/MA0GCSqGSIb3DQEBBQUAMIGHMQswCQYD
VQQGEwJUVzEPMA0GA1UECBMGVGFpd2FuMRAwDgYDVQQHEwdIc2luQ2h1MQ4wDAYD
VQQKEwVaeVhFTDEMMAoGA1UECxMDTVNHMRQwEgYDVQQDEwtaeVhFTFJvb3RDQTEh
MB8GCSqGSIb3DQEJARYSenl4ZWxAenl4ZWwuY29tLnR3MB4XDTEwMDUxODE1MDgz
NFoXDTMwMDUxODE1MDgzNFowgYsxCzAJBgNVBAYTAlRXMQ8wDQYDVQQIEwZUYWI3
YW4xEDAOBgNVBAcTB0hzaW5DaHUxDjAMBgNVBAoTBVp5WEVMMQwwCgYDVQQLEwNN
U0cxGDAWBgNVBAMTD1p5WEVMTW9kZW0uSG9tZTEhMB8GCSqGSIb3DQEJARYSenl4
ZWxAenl4ZWwuY29tLnR3MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
thPSIYnw9YpbQw2JC5FtpigGXc+GGgxO1ns7+tpwndkLDBfBE/YXWQDd1CGe1wUX
```

Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAthPSIYnw9YpbQw2JC5FtpigGXc+GGgxO1ns7+tpwndkLDBfB
E/YXWQDd1CGe1wUX98CGqXOWjTbtpI0m8bht7JCZCoeAcYFFtrOWe69WxZU0IsL+
DaUOqxERNjRKjx84BFxvHnA9R8yOSsZWbxHZRXVVil8Vfg5IBUPN1jK3M74n3J7D
0UCAA8FU7BuMQxkdxIB4snIAgu6aZHQssMrmkS670y2qDAMQxudCo+5t94P0ADsR
YcAOa7w7nPbuqic+u1Jrzx4pQwDY3hIB8etNf2UG0jstjUvy2SO+Qg+AxhbOBygu
GXiWPxjw8fhANrKbv3QXkfnX5b4QaQnJNNZgMQIDAQABAoIBAQCdzRpCbhW+yJWF
zJJMy1KLob66ySPBKY+eRZnbNDxMIZJ4fZHh2fOsOJslwcanNgvqtho/fCUr6ElZ
YDxjXGMwIrV8sak5Nj+UM5sIQPZkMYctbnu+maHX0ufm4XUJC5aB+RZ4+++wbXGZ
DsJUatSyZRmo3fWDIbgp0vTvQm8S0LGuLGx8Rw3iomDHujU8ruxLMDVDZCbo9+Y5
```

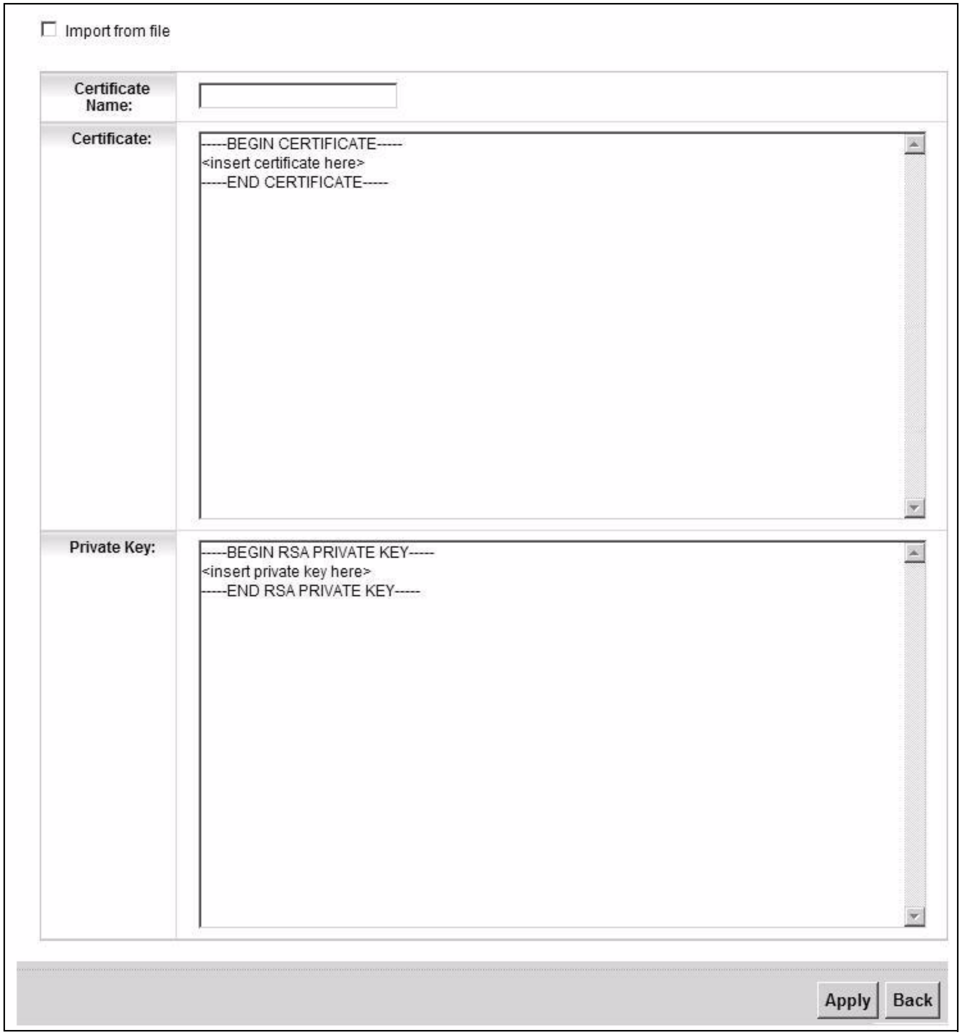
Signing Request

12.3.2 Import Certificate

Click **Security Settings > Local Certificates** and then **Import Certificate** to open the **Import Local Certificate** screen. Follow the instructions in this screen to save an existing certificate to the ZyXEL Device.

Note: You must remove any spaces from the certificate's filename before you can import it.

Figure 67 Import Local Certificate



☐ Import from file

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

The following table describes the labels in this screen.

Table 47 Import Local Certificate

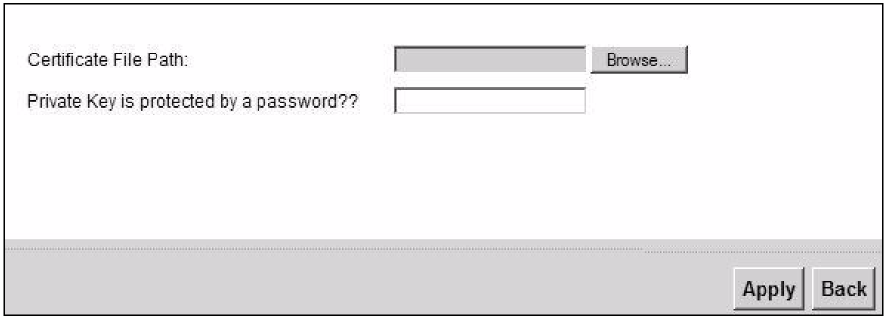
LABEL	DESCRIPTION
Import from file	Click this check box to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Certificate	Copy and paste the certificate into the text box to store it on the ZyXEL Device.
Private Key	Copy and paste the private key into the text box to store it on the ZyXEL Device.

Table 47 Import Local Certificate (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

If you click **Import from file** in the **Import Local Certificate** screen, the following screen is displayed.

Figure 68 Import Local Certificate > Import from file



Certificate File Path:

Private Key is protected by a password??

The following table describes the labels in this screen.

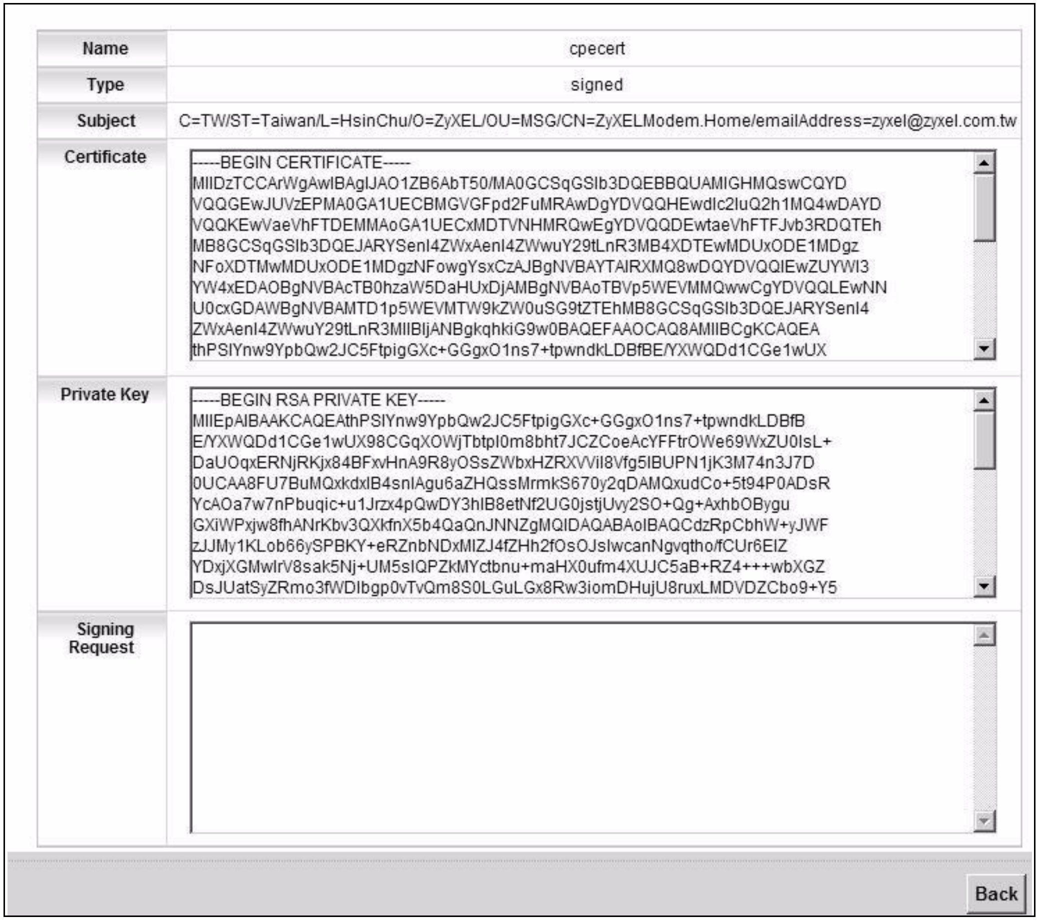
Table 48 Import Local Certificate > Import from file

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the certificate you want to upload in this field or click **Browse ...** to find it.
Private Key is protected by a password?	Enter the private key into the text box to store it on the ZyXEL Device. The private key should not exceed 63 ASCII characters (not including spaces).
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

12.3.3 Certificate Details

Click **Security Settings> Certificates > Local Certificates** to open the **My Certificates** screen. Click the **View** icon to open the **Certificate Details** screen. Use this screen to view in-depth certificate information and change the certificate's name.

Figure 69 Certificate Details



Name	cpecert
Type	signed
Subject	C=TW/ST=Taiwan/L=HsinChu/O=ZyXEL/OU=MSG/CN=ZyXELModem.Home/emailAddress=zyxel@zyxel.com.tw

Certificate

```
-----BEGIN CERTIFICATE-----
MIIDzTCCArWgAwIBAgIJAO1ZB6AbT50/MA0GCSqGSIb3DQEBBQUAMIGHMQswCQYD
VQQGEwJUVzEPMA0GA1UECBMGVGFpd2FuMRAwDgYDVQQHEwdIc2luQ2h1MQ4wDAYD
VQQKEwVaeVhFTDEMMAoGA1UECxMDTVNHMRQwEgYDVQQDEwtaeVhFTFJvb3RDQTEh
MB8GCSqGSIb3DQEJARYSenl4ZWxAenl4ZWwuY29tLnR3MB4XDTEwMDUxODE1MDgz
NFoXDTMwMDUxODE1MDgzNFowgYsxCzAJBgNVBAYTAlRXMQ8wDQYDVQQIEwZUYWl3
YW4xEDAOBgNVBAcTB0hzaW5DaHUxDjAMBgNVBAoTBVp5WEVMMQwwCgYDVQQLEwNN
U0cxGDAWBgNVBAMTD1p5WEVMTW9kZW0uSG9tZTEhMB8GCSqGSIb3DQEJARYSenl4
ZWxAenl4ZWwuY29tLnR3MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
thPSIYnw9YpbQw2JC5FtpigGXc+GGgxO1ns7+tpwndkLDBfBE/YXWQDd1CGe1wUX
```

Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAthPSIYnw9YpbQw2JC5FtpigGXc+GGgxO1ns7+tpwndkLDBfB
E/YXWQDd1CGe1wUX98CGqXOWjTbtpI0m8bht7JCZCoeAcYFFtrOWe69WxZU0IsL+
DaUOqxERNjRKjx84BFxvHnA9R8yOSsZWbxHZRXVVil8Vfg5IBUPN1jK3M74n3J7D
0UCAA8FU7BuMQxkdxIB4snIAgu6aZHQssMrmkS670y2qDAMQxudCo+5t94P0ADsR
YcAOa7w7nPbuqic+u1Jrzx4pQwDY3hIB8etNf2UG0jstjUvy2SO+Qg+AxhbOBygu
GXiWPxjw8fhANrKbv3QXkfnX5b4QaQnJNNZgMQIDAQABAoIBAQCdzRpCbhW+yJWF
zJJMy1KLob66ySPBKY+eRZnbNDxMIZJ4fZHh2fOsOJsIwcanNgvqtho/fCUr6EIZ
YDxjXGMwIrV8sak5Nj+UM5sIQPZkMYctbnu+maHX0ufm4XUJC5aB+RZ4+++wbXGZ
DsJUatSyZRmo3fWDIbgp0vTvQm8S0LGuLGx8Rw3iomDHujU8ruxLMDVDZCbo9+Y5
```

Signing Request

The following table describes the labels in this screen.

Table 49 Certificate Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 63 characters to identify this certificate. You may use any character (not including spaces).
Type	This field displays general information about the certificate. **signed** means that a Certification Authority signed the certificate. **request** means this is a certification request.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organization (O), State (ST) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. This displays **null** in a certification request. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).

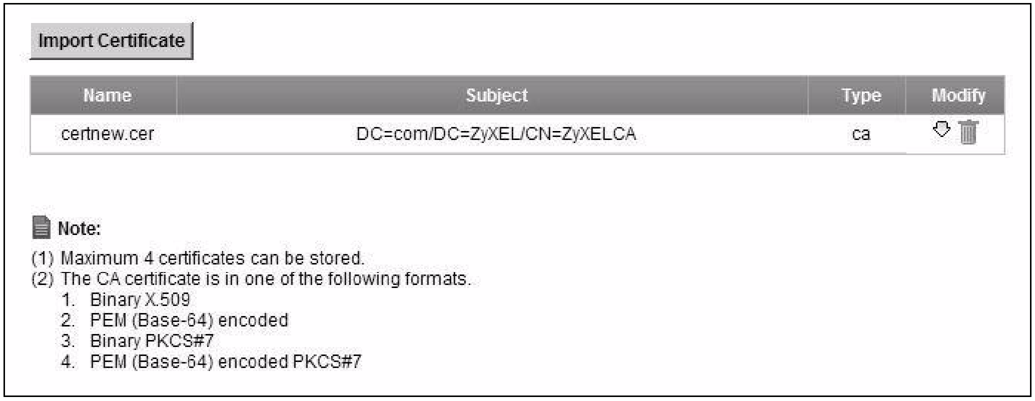
Table 49 Certificate Details (continued)

LABEL	DESCRIPTION
Private Key	This read-only text box displays the private key in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the private key into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Signing Request	This read-only text box displays the request information in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. This displays **null** in a signed certificate.
Back	Click **Back** to return to the previous screen.

12.4 The Trusted CA Screen

Click **Security Settings > Certificates > Trusted CA** to open the following screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 70 Security Settings > Certificates > Trusted CA



Name	Subject	Type	Modify
certnew.cer	DC=com/DC=ZyXEL/CN=ZyXELCA	ca	

Note:
(1) Maximum 4 certificates can be stored.
(2) The CA certificate is in one of the following formats.
1. Binary X.509
2. PEM (Base-64) encoded
3. Binary PKCS#7
4. PEM (Base-64) encoded PKCS#7

The following table describes the fields in this screen.

Table 50 Security Settings > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the ZyXEL Device.
Name	This field displays the name used to identify this certificate.

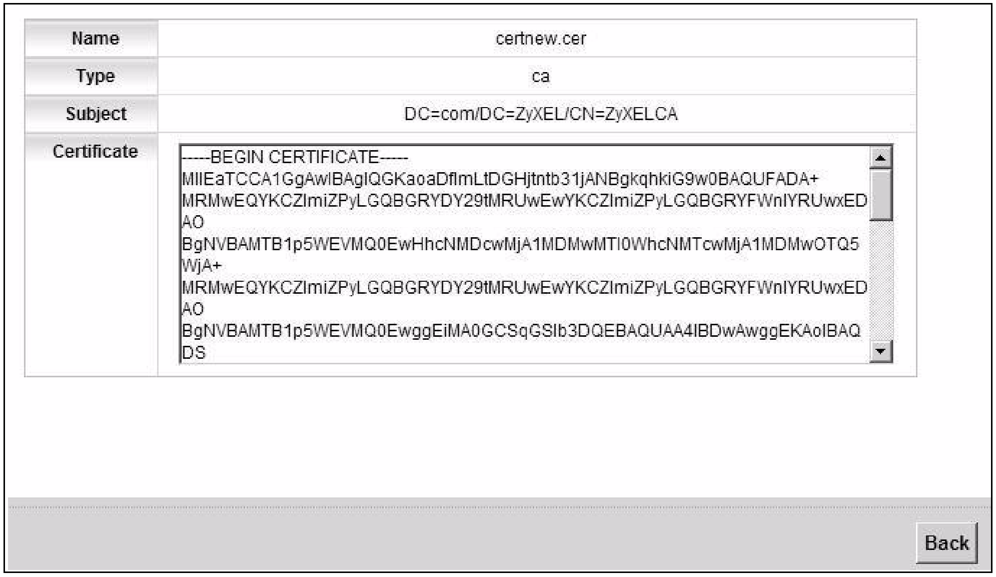
Table 50 Security Settings > Certificates > Trusted CA (continued)

LABEL	DESCRIPTION
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Modify	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Delete** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

12.4.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate.

Figure 71 Trusted CA: View



Name	certnew.cer
Type	ca
Subject	DC=com/DC=ZyXEL/CN=ZyXELCA
Certificate	

```
-----BEGIN CERTIFICATE-----
MIIEaTCCA1GgAwIBAgIQGKaoaDflmLtDGHjtntb31jANBgkqhkiG9w0BAQUFADA+
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFWnlYRUwxED
AO
BgNVBAMTB1p5WEVMQ0EwHhcNMDcwMjA1MDMwMTI0WhcNMTcwMjA1MDMwOTQ5
WjA+
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFWnlYRUwxED
AO
BgNVBAMTB1p5WEVMQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQ
DS
```

The following table describes the fields in this screen.

Table 51 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.

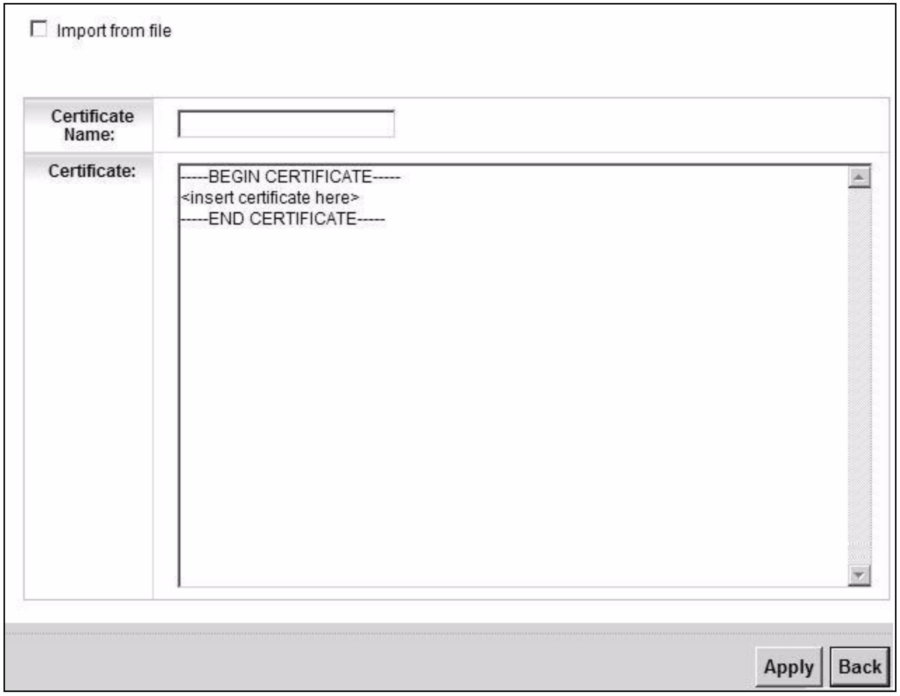
Table 51 Trusted CA: View (continued)

LABEL	DESCRIPTION
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click **Back** to return to the previous screen.

12.4.2 Import Trusted CA Certificate

Click the **Import Certificate** button in the **Trusted CA** screen to open the following screen. The ZyXEL Device trusts any valid certificate signed by any of the imported trusted CA certificates.

Figure 72 Trusted CA: Import Certificate



□ Import from file

Certificate Name:	
Certificate:	-----BEGIN CERTIFICATE----- <insert certificate here> -----END CERTIFICATE-----

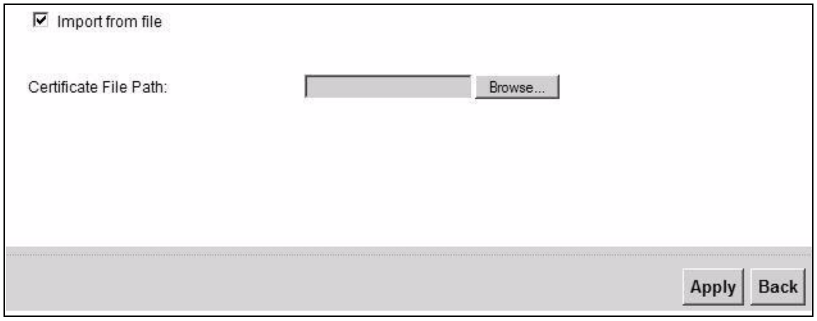
The following table describes the fields in this screen.

Table 52 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Import from file	Click this check box to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.
Certificate Name	Enter the name that identifies this certificate. The certificate name should not exceed 63 ASCII characters (not including spaces).
Certificate	Copy and paste the certificate into the text box to store it on the ZyXEL Device.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

If you click **Import from file** in the **Import Local Certificate** screen, the following screen is displayed.

Figure 73 Trusted CA: Import Certificate > Import from file



☑ Import from file

Certificate File Path:

The following table describes the labels in this screen.

Table 53 Import Local Certificate

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the certificate you want to upload in this field or click **Browse ...** to find it.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

13

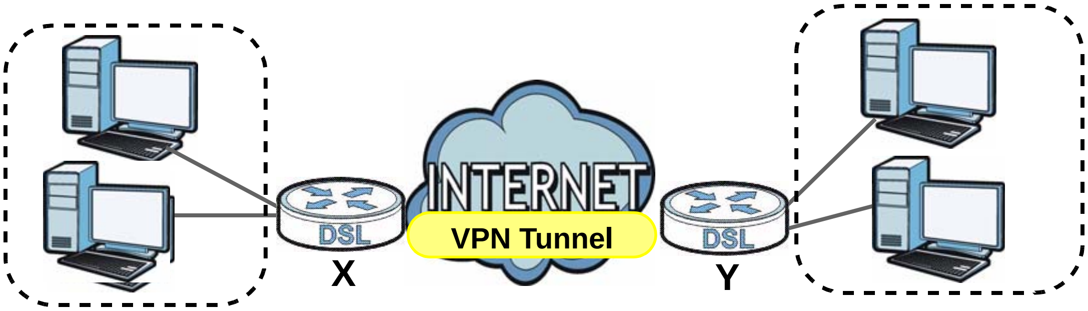
IPSec

13.1 Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer. The following figure is an example of an IPSec VPN tunnel.

Figure 74 VPN: Example



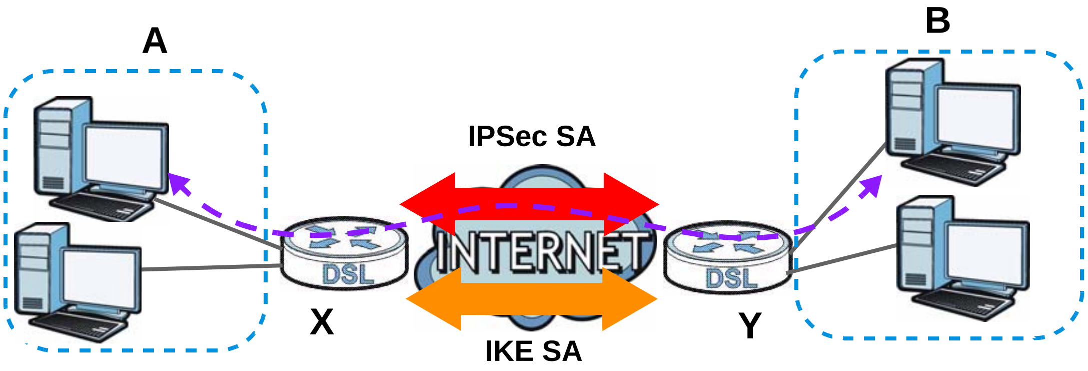
13.1.1 What You Can Do in this Chapter

- Use the **Settings** screen to view the configured IPSec policies and add, edit or remove a policy (Section 13.2 on page 179).
- Use the **Status** screen to display and manage the current active VPN connections (Section 13.3 on page 188).

13.1.2 What You Need to Know

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyXEL Device and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyXEL Device and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the ZyXEL Device and remote IPSec router can send data between computers on the local network and remote network. The following figure illustrates this.

Figure 75 VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is established securely using the IKE SA that routers **X** and **Y** established first.

Remote IPSec Gateway Address

Remote IPSec Gateway Address is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Remote IPSec Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Remote IPSec Gateway Address** field.

You can also enter a remote secure gateway's domain name in the **Remote IPSec Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The ZyXEL Device has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

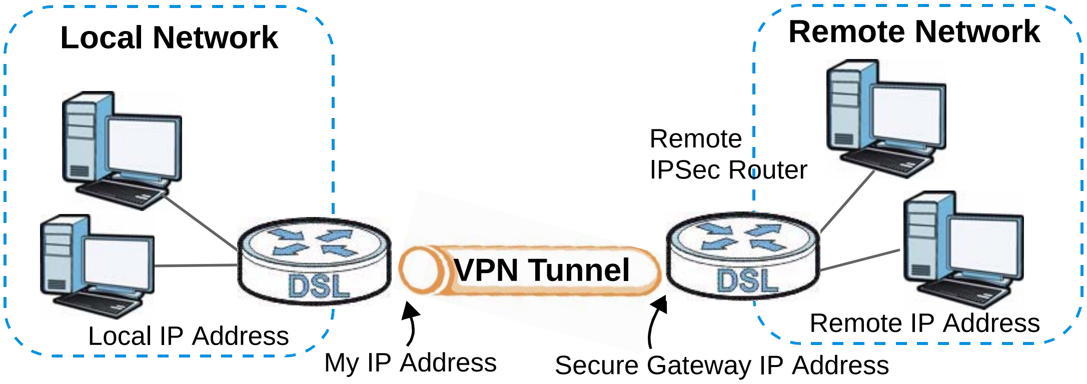
Finding Out More

See Section 13.4 on page 188 for advanced technical information on IPSec VPN.

13.2 The IPSec Settings Screen

The following figure helps explain the main fields in the web configurator.

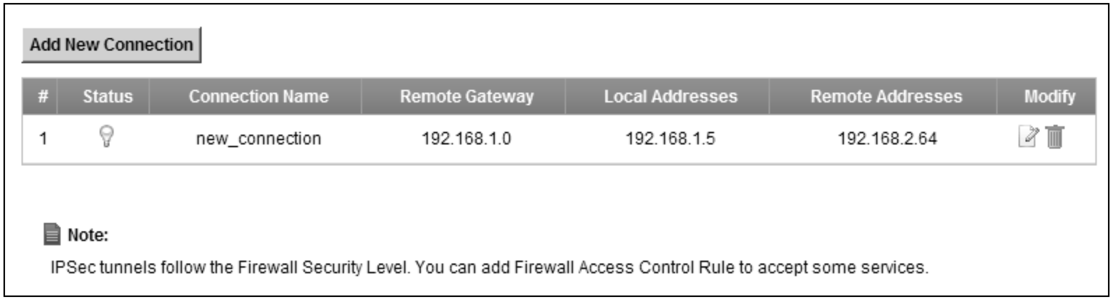
Figure 76 IPSec Summary Fields



Local and remote IP addresses must be static.

Click **Security Settings** > **IPSec** to open the **Settings** screen. This is a menu of your IPSec tunnels.

Figure 77 Security Settings > IPSec > Settings



#	Status	Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Modify
1	💡	new_connection	192.168.1.0	192.168.1.5	192.168.2.64	✎ 🗑

Note:
IPSec tunnels follow the Firewall Security Level. You can add Firewall Access Control Rule to accept some services.

The following table describes the fields in this screen.

Table 54 Security Settings > IPSec > Settings

LABEL	DESCRIPTION
Add New Connection	Click this to configure a new VPN policy.
#	This is the index number of the entry.

Table 54 Security Settings > IPSec > Settings (continued)

LABEL	DESCRIPTION
Status	This field displays whether the VPN policy is active or not. A yellow bulb signifies that this VPN policy is active. A gray bulb signifies that this VPN policy is not active.
Connection Name	This field displays the identification name for this VPN policy.
Remote Gateway	This is the static WAN IP address or URL of the remote IPSec router.
Local Addresses	This is the IP address of computer(s) on your local network behind your ZyXEL Device.
Remote Addresses	This is the IP address of computer(s) on the remote network behind the remote IPSec router.
Modify	Click the **Edit** icon to edit the VPN configuration. Click the **Delete** icon to remove an existing VPN configuration.

13.2.1 Add/Edit IPSec Setting

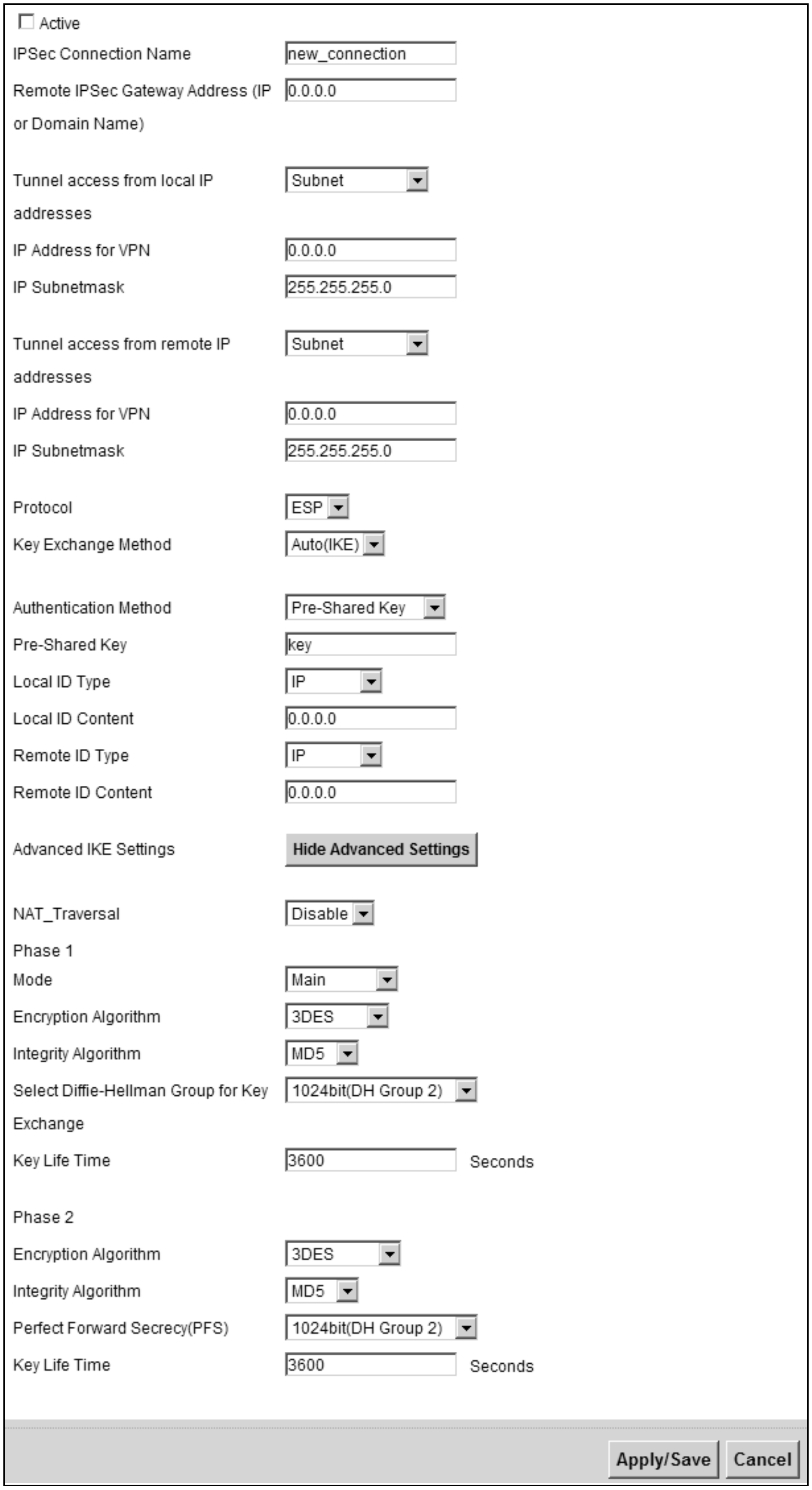
Click **Add New Connection** or a policy's **Edit** icon in the **IPSec > Settings** screen to edit VPN policies.

Note: The ZyXEL Device uses the system default gateway interface's WAN IP address as its WAN IP address to set up a VPN tunnel.

13.2.1.1 Auto(IKE) Key Setup

Auto(IKE) provides more protection so it is generally recommended. You only configure VPN manual key when you select **Auto(IKE)** in the **Key Exchange Method** field on the **IPSec > Setting: Add/Edit** screen. The following is the **IPSec Setting - Auto(IKE)** screen.

Figure 78 Settings > Add/Edit: Auto(IKE)



□ Active

IPSec Connection Name	new_connection	
Remote IPSec Gateway Address (IP or Domain Name)	0.0.0.0	
Tunnel access from local IP addresses	Subnet	
IP Address for VPN	0.0.0.0	
IP Subnetmask	255.255.255.0	
Tunnel access from remote IP addresses	Subnet	
IP Address for VPN	0.0.0.0	
IP Subnetmask	255.255.255.0	
Protocol	ESP	
Key Exchange Method	Auto(IKE)	
Authentication Method	Pre-Shared Key	
Pre-Shared Key	key	
Local ID Type	IP	
Local ID Content	0.0.0.0	
Remote ID Type	IP	
Remote ID Content	0.0.0.0	
Advanced IKE Settings	Hide Advanced Settings	
NAT_Traversal	Disable	
Phase 1		
Mode	Main	
Encryption Algorithm	3DES	
Integrity Algorithm	MD5	
Select Diffie-Hellman Group for Key Exchange	1024bit(DH Group 2)	
Key Life Time	3600	Seconds
Phase 2		
Encryption Algorithm	3DES	
Integrity Algorithm	MD5	
Perfect Forward Secrecy(PFS)	1024bit(DH Group 2)	
Key Life Time	3600	Seconds

The following table describes the fields in this screen.

Table 55 Settings > Add/Edit: Auto(IKE)

LABEL	DESCRIPTION
Enable	Select this check box to activate this VPN policy. This option determines whether a VPN rule is applied before a packet leaves the firewall.
IPSec Connection Name	Type up to 39 alphanumeric characters to identify this VPN policy. You may use spaces, underscores and dashes, but the ZyXEL Device drops trailing spaces.
Remote IPSec Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Tunnel access from local IP addresses	Specify the IP addresses of the devices behind the ZyXEL Device that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. Use the drop-down list box to choose **Single Address** or **Subnet**. Select **Single Address** for a single IP address. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address for VPN	When the local IP address type is configured to **Single Address**, enter a (static) IP address on the LAN behind your ZyXEL Device. When the local IP address type is configured to **Subnet**, enter a (static) IP address on the LAN behind your ZyXEL Device.
IP Subnet mask	When the local IP address type is configured to **Single Address**, this field is not available. When the local IP address type is configured to **Subnet**, enter a subnet mask on the LAN behind your ZyXEL Device.
Tunnel access from remote IP addresses	Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. Use the drop-down list box to choose **Single Address** or **Subnet**. Select **Single Address** with a single IP address. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address for VPN	When the remote IP address type is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the remote IP address type is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router.

Table 55 Settings > Add/Edit: Auto(IKE) (continued)

LABEL	DESCRIPTION
IP Subnetmask	When the remote IP address type is configured to **Single Address**, this field is not available. When the remote IP address type is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
Protocol	This field displays **ESP** and the ZyXEL Device uses ESP (Encapsulation Security Payload) for VPN. The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**.
Key Exchange Method	Select **Auto(IKE)** or **Manual** from the drop-down list box. **Auto(IKE)** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **Auto(IKE)** key management.
Authentication Method	Select **Pre-Shared Key** to use a pre-shared key for authentication. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Select **Certificates (X.509)** to use a certificate for authentication.
Pre-Shared Key	This field is available only when you select **Pre-Shared Key** in the **Authentication Method** field. Type up to 15 alphanumeric characters for the pre-shared key. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a “PYLD_MALFORMED” (payload malformed) packet if the same pre-shared key is not used on both ends.
Local/Remote ID Type	Select **IP** to identify this ZyXEL Device by its IP address. Select **DNS** to identify this ZyXEL Device by a domain name. Select **E-mail** to identify this ZyXEL Device by an e-mail address. Select **ASN1DN** (Abstract Syntax Notation one - Distinguished Name) to identify the remote IPSec router by the subject field in a certificate. This is used only with certificate-based authentication.
Local/Remote ID Content	When you select **IP** in the **Local/Remote ID Type** field, type the IP address of your computer in the **Local/Remote ID Content** field. When you select **DNS** or **E-mail** in the **Local/Remote ID Type** field, type a domain name or e-mail address by which to identify this ZyXEL Device in the **Local/Remote ID Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Advanced IKE Settings	Click **Show Advanced Settings** to display and configure more detailed settings of your IKE key management. Otherwise, click **Hide Advanced Settings**.
NAT_Traversal	Select **Enable** if you want to set up a VPN tunnel when there are NAT routers between the ZyXEL Device and remote IPSec router. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward UDP port 500 packets to the remote IPSec router behind the NAT router. Otherwise, select **Disable**.
Phase 1/Phase 2	

Table 55 Settings > Add/Edit: Auto(IKE) (continued)

LABEL	DESCRIPTION
Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	Select **DES**, **3DES**, **AES-128**, **ES-192** or **AES-256** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit, 192-bit or 256-bit key. **AES** is faster than **3DES**.
Integrity Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA1** for maximum security.
Select Diffie-Hellman Group for Key Exchange	You must choose a key group for key exchange in SA setup. **768bit** refers to Diffie-Hellman Group 1 a 768 bit random number. **1024bit** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. Other options include **1536**, **2048**, and **3072** bit Diffie-Hellman groups.
Key Life Time (Seconds)	Define the length of time before an IKE or IPSec SA automatically renegotiates in this field. It may range from 1 to 2,000,000,000 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Apply/Save	Click **Apply/Save** to save your changes and return to the **IPSec** screen.
Cancel	Click **Cancel** to exit this screen without saving.

13.2.1.2 Manual Key Setup

Manual key management is useful if you have problems with **Auto(IKE)** key management.

13.2.1.3 Security Parameter Index (SPI)

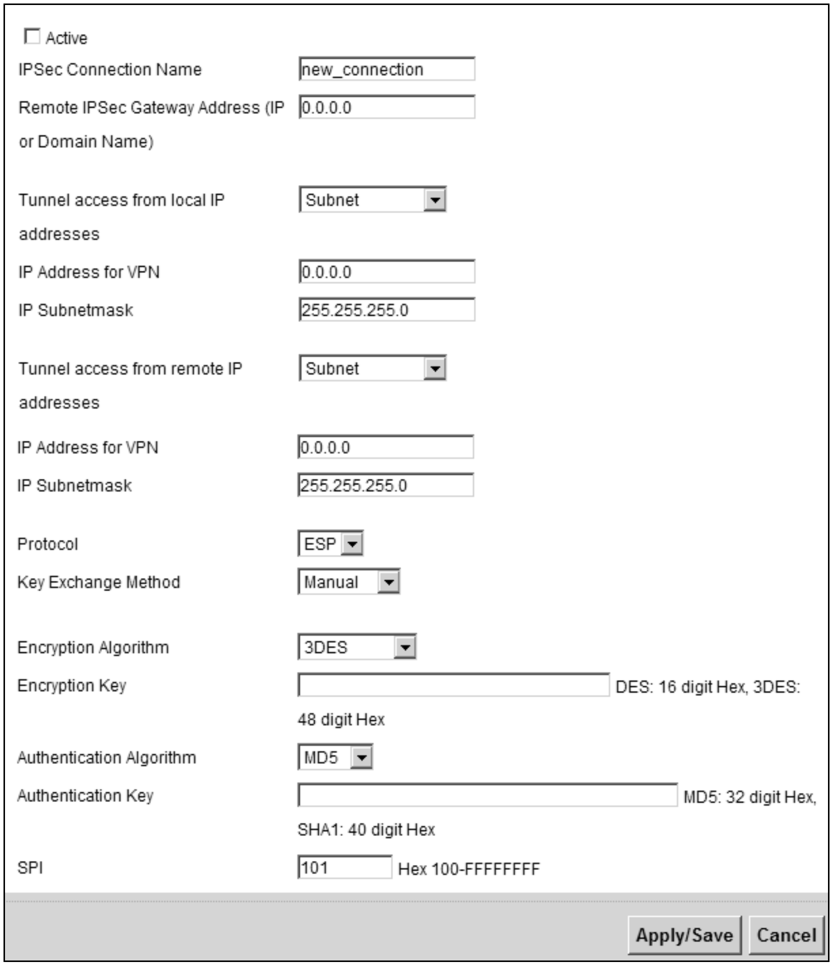
An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

13.2.2 Configuring Manual Key

You only configure VPN manual key when you select **Manual** in the **Key Exchange Method** field on the **IPSec > Setting: Add/Edit** screen. The following is the **IPSec Setting - Manual** screen.

Figure 79 Settings > Add/Edit: Manual



□ Active

IPSec Connection Name	new_connection
Remote IPSec Gateway Address (IP or Domain Name)	0.0.0.0
Tunnel access from local IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Tunnel access from remote IP addresses	Subnet
IP Address for VPN	0.0.0.0
IP Subnetmask	255.255.255.0
Protocol	ESP
Key Exchange Method	Manual
Encryption Algorithm	3DES
Encryption Key	DES: 16 digit Hex, 3DES: 48 digit Hex
Authentication Algorithm	MD5
Authentication Key	MD5: 32 digit Hex, SHA1: 40 digit Hex
SPI	101 Hex 100-FFFFFFFF

The following table describes the fields in this screen.

Table 56 IPSec Settings > Add/Edit: Manual

LABEL	DESCRIPTION
Enable	Select this check box to activate this VPN policy. This option determines whether a VPN rule is applied before a packet leaves the firewall.
IPSec Connection Name	Type up to 39 alphanumeric characters to identify this VPN policy. You may use spaces, underscores and dashes, but the ZyXEL Device drops trailing spaces.
Remote IPSec Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Tunnel access from local IP addresses	Specify the IP addresses of the devices behind the ZyXEL Device that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. Use the drop-down list box to choose **Single Address** or **Subnet**. Select **Single Address** for a single IP address. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address for VPN	When the local IP address type is configured to **Single Address**, enter a (static) IP address on the LAN behind your ZyXEL Device. When the local IP address type is configured to **Subnet**, enter a (static) IP address on the LAN behind your ZyXEL Device.
IP Subnetmask	When the local IP address type is configured to **Single Address**, this field is not available. When the local IP address type is configured to **Subnet**, enter a subnet mask on the LAN behind your ZyXEL Device.
Tunnel access from remote IP addresses	Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. Use the drop-down list box to choose **Single Address** or **Subnet**. Select **Single Address** with a single IP address. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address for VPN	When the remote IP address type is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the remote IP address type is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router.

Table 56 IPSec Settings > Add/Edit: Manual (continued)

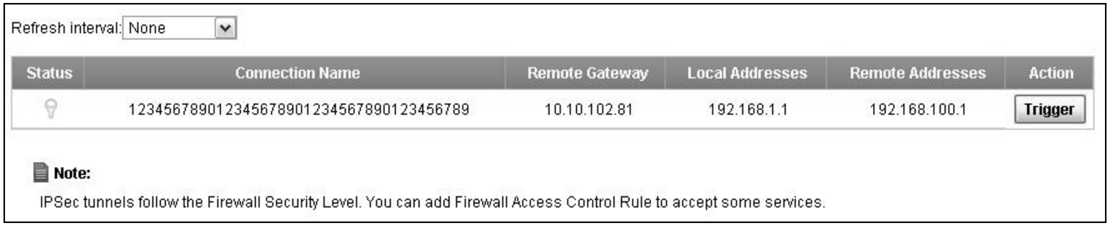
LABEL	DESCRIPTION
IP Subnetmask	When the remote IP address type is configured to **Single Address**, this field is not available. When the remote IP address type is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
Protocol	This field displays **ESP** and the ZyXEL Device uses ESP (Encapsulation Security Payload) for VPN. The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**.
Key Exchange Method	Select **Auto(IKE)** or **Manual** from the drop-down list box. **Auto(IKE)** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **Auto(IKE)** key management.
Encryption Algorithm	Select **DES**, **3DES**, **AES(aes-cbc)** or **ESP_NULL** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES(aes-cbc)** in Cipher Block Chaining (CBC) mode uses a 128-bit key. **AES** is faster than **3DES**. Select **ESP_NULL** to set up a tunnel without encryption. When you select **ESP_NULL**, you do not enter an encryption key.
Encryption Key	Type 16 hexadecimal ("0-9", "A-F") characters if you select to use the DES encryption algorithm or 48 hexadecimal characters if you use the 3DES encryption algorithm.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA1** for maximum security.
Authentication Key	Type 32 hexadecimal ("0-9", "A-F") characters if you select to use the MD5 authentication algorithm or 40 hexadecimal characters if you use the SHA1 authentication algorithm.
SPI	Type a hexadecimal number from 111 to FFFFFFFF for the Security Parameter Index.
Apply/Save	Click **Apply/Save** to save your changes and return to the **IPSec** screen.
Cancel	Click **Cancel** to exit this screen without saving.

13.3 The IPSec Status Screen

Click **Security Settings** > **IPSec** > **Status** to open the screen as shown. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. The following table describes the fields in this tab.

Figure 80 Security Settings > IPSec > Status



Refresh interval: None

Status	Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Action
	1234567890123456789012345678901234567890123456789	10.10.102.81	192.168.1.1	192.168.100.1	Trigger

Note:

IPSec tunnels follow the Firewall Security Level. You can add Firewall Access Control Rule to accept some services.

The following table describes the fields in this screen.

Table 57 Security Settings > IPSec > Status

LABEL	DESCRIPTION
Refresh Interval	Select how often the screen should be refreshed from the drop-down list box.
Status	This field displays whether the VPN connection is up (a yellow bulb) or down (a gray bulb).
Connection Name	This field displays the identification name for this VPN policy.
Remote Gateway	This is the static WAN IP address or URL of the remote IPSec router.
Local Addresses	This is the IP address of computer(s) on your local network behind your ZyXEL Device.
Remote Addresses	This is the IP address of computer(s) on the remote network behind the remote IPSec router.
Action	Click **Trigger** to establish a VPN connection with the remote network.

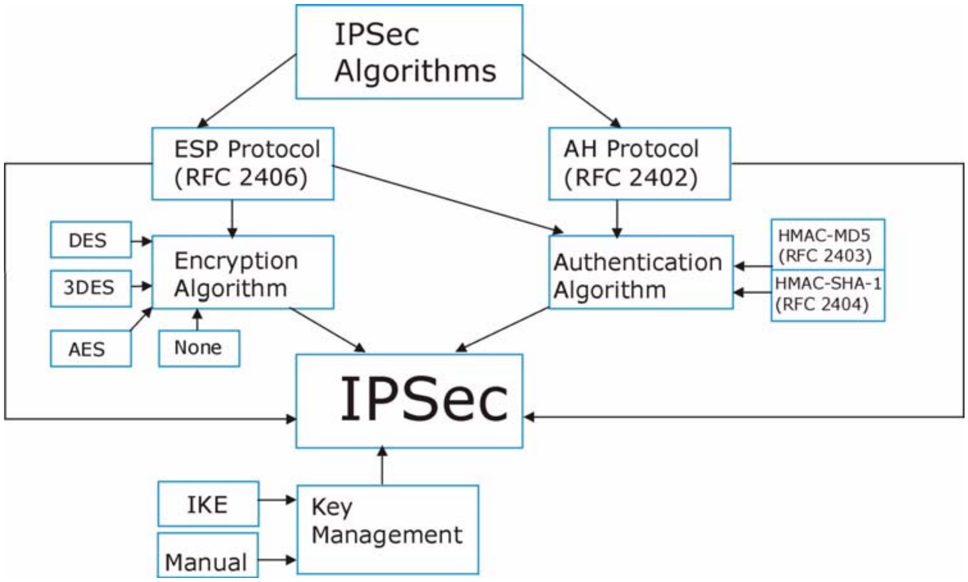
13.4 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

13.4.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 81 IPSec Architecture



IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols.

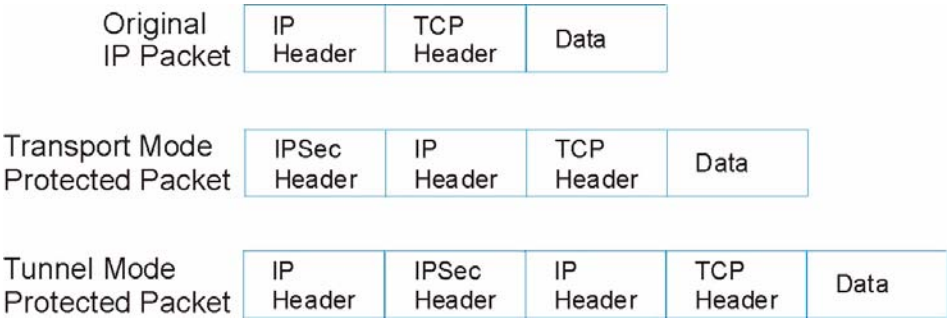
Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

13.4.2 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode. At the time of writing, the ZyXEL Device supports **Tunnel** mode only.

Figure 82 Transport and Tunnel Mode IPSec Encapsulation



Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel Mode

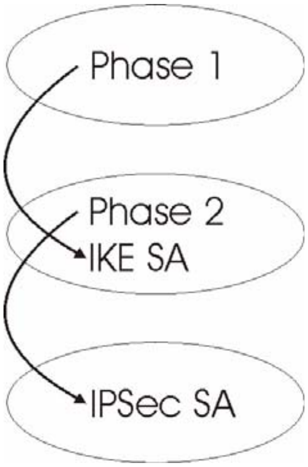
Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

13.4.3 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 83 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The ZyXEL Device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

13.4.4 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

13.4.5 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the ZyXEL Device.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 58 VPN and NAT

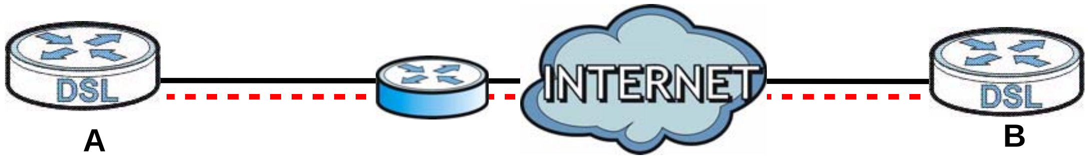
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

13.4.6 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the ZyXEL Device's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 84 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In the above figure, when IPSec router **A** tries to establish an IKE SA, IPSec router **B** checks the UDP port 500 header, and IPSec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 59 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

Y* - This is supported in the ZyXEL Device if you enable NAT traversal.

13.4.7 ID Type and Content

With aggressive negotiation mode (see Section 13.4.4 on page 192), the ZyXEL Device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the ZyXEL Device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses.

Regardless of the ID type and content configuration, the ZyXEL Device does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see Section 13.4.4 on page 192), the ID type and content are encrypted to provide identity protection. In this case the ZyXEL Device can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The ZyXEL Device can distinguish up to 48 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and eight key groups when you configure a VPN rule (see Section 13.2 on page 179). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 60 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer.
DNS	Type a domain name (up to 31 characters) by which to identify this ZyXEL Device.

Table 60 Local ID Type and Content Fields (continued)

LOCAL ID TYPE=	CONTENT=
E-mail	Type an e-mail address (up to 31 characters) by which to identify this ZyXEL Device.
	The domain name or e-mail address that you use in the **Local ID Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

13.4.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two ZyXEL Devices in this example can complete negotiation and establish a VPN tunnel.

Table 61 Matching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Remote ID type: IP	Remote ID type: E-mail
Remote ID content: 1.1.1.2	Remote ID content: tom@yourcompany.com

The two ZyXEL Devices in this example cannot complete their negotiation because ZyXEL Device B’s **Local ID type** is **IP**, but ZyXEL Device A’s **Remote ID type** is set to **E-mail**. An “ID mismatched” message displays in the IPSEC LOG.

Table 62 Mismatching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.2
Remote ID type: E-mail	Remote ID type: IP
Remote ID content: aa@yahoo.com	Remote ID content: 1.1.1.0

13.4.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 13.4.3 on page 191 for more on IKE phases). It is called “pre-shared” because you have to share it with another party before you can communicate with them over a secure connection.

13.4.9 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit, 1024-bit 1536-bit, 2048-bit, and 3072-bit Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

14

Parental Control

14.1 Overview

Parental control allows you to permit or block certain web sites to home network computers.

You can define time periods and days during which the ZyXEL Device performs parental control on a specific user in the **Advanced > Scheduler Rules** screen (see Chapter 20 on page 239 for detailed information).

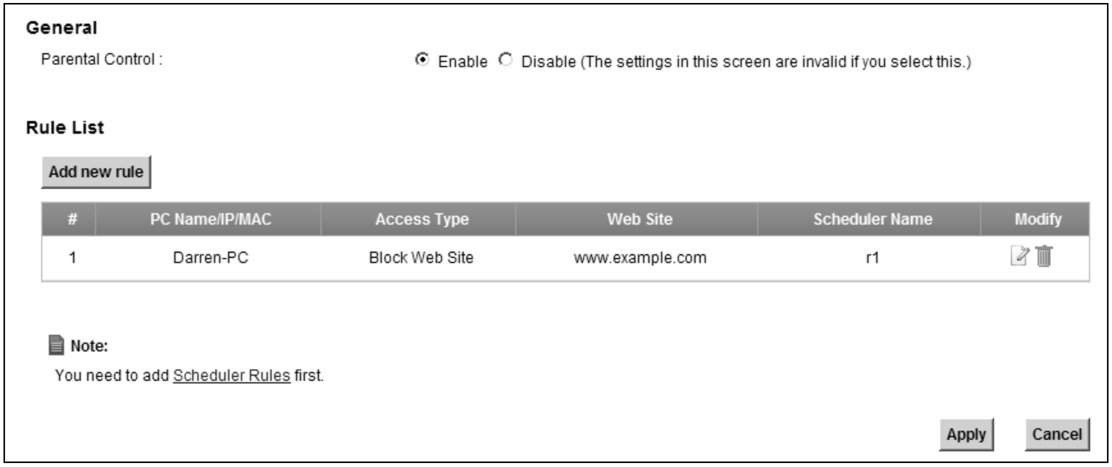
14.2 The Parental Control Screen

Use this screen to configure parental control settings to block the users on your network from accessing certain web sites.

Click **Parental Control** to open the following screen.

Note: You must configure a scheduler rule in the **Advanced > Scheduler Rule** screen before the parental control function can be enabled. Click **Scheduler Rule** in the note to go to the **Scheduler Rule** screen for configurations.

Figure 85 Parental Control



General

Parental Control : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Rule List

#	PC Name/IP/MAC	Access Type	Web Site	Scheduler Name	Modify
1	Darren-PC	Block Web Site	www.example.com	r1	

Note:
You need to add Scheduler Rules first.

The following table describes the fields in this screen.

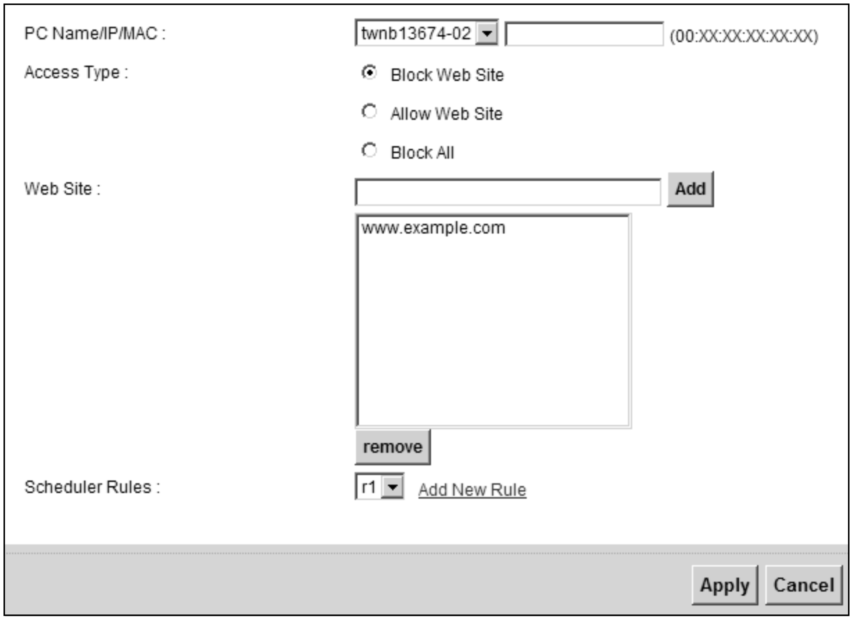
Table 63 Parental Control

LABEL	DESCRIPTION
Add new rule	Click this to create a new parental control rule.
#	This is the index number of the rule.
PC Name/IP/MAC	The ZyXEL Device allows or prohibits the users from viewing the Web sites with the URLs listed below.
Access Type	This shows the access type that is applied on the user to the web site of this rule.
Web Site	This is the URL of the web site in this rule.
Scheduler Name	This is the name of the schedule rule that is applied.
Modify	Click the **Edit** icon to edit the rule. Click the **Delete** icon to delete an existing rule.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

14.2.1 Add/Edit Parental Control Rule

Click **Add new rule** in the **Parental Control** screen or click the **Edit** icon next to a rule to open the following screen.

Figure 86 Parental Control: Add/Edit



PC Name/IP/MAC : twnb13674-02 (00:XX:XX:XX:XX:XX)

Access Type : ● Block Web Site ○ Allow Web Site ○ Block All

Web Site : www.example.com

Scheduler Rules : r1

The following table describes the fields in this screen.

Table 64 Parental Control: Add/Edit

LABEL	DESCRIPTION
PC Name/IP/MAC	Select the user that you want to apply this rule to from the drop-down list box. If you want to add an user that is not listed, select **User Defined** and enter its MAC address. This field is read-only if you are editing the parental control rule.
Access Type	Select the access type that is applied on the user to the web site of this rule. If you select **Block Web Site**, the ZyXEL Device prohibits the users from viewing the web sites with the URLs listed below. If you select **Allow Web Site**, the ZyXEL Device blocks access to all URLs except ones listed below. If you select **Block All**, the ZyXEL Device blocks access to all URLs.
Web Site	Enter the URL of web site to which the ZyXEL Device blocks or allows access. Click **Add** to add this URL to the list below.
Remove	Select an URL from the list and click **Remove** to delete it.
Scheduler Rule	Select the scheduler rule that you want to apply from the drop-down list box. If you have not configured a scheduler rule or want to add a new one, click the **Add New Rule** button to go to the **Scheduler Rule** screen. See Chapter 20 on page 239 for more information.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

15

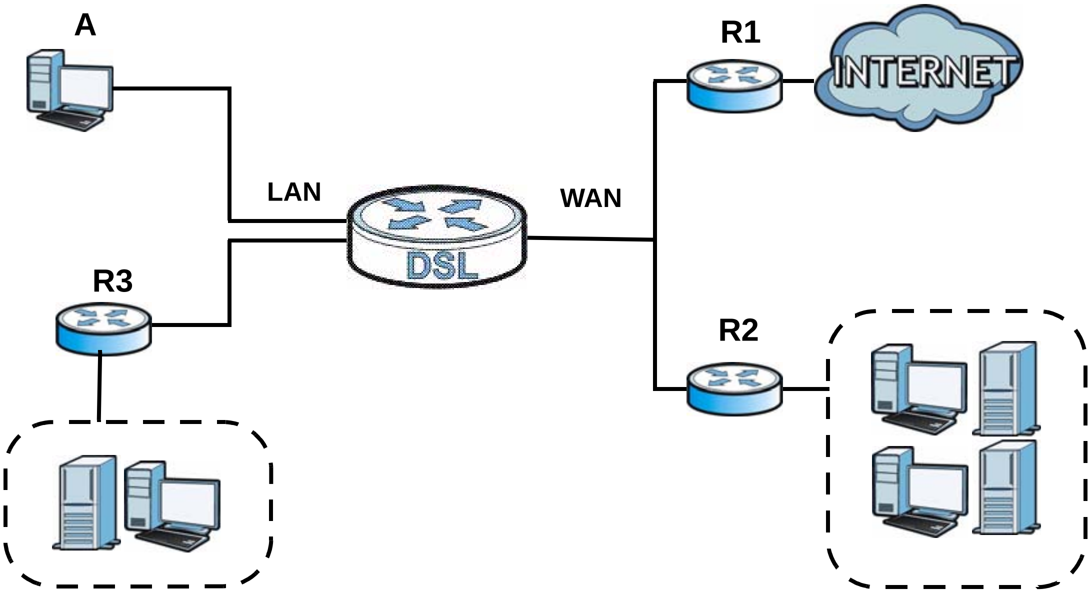
Routing

15.1 Overview

The ZyXEL Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the ZyXEL Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the ZyXEL Device's LAN interface. The ZyXEL Device routes most traffic from **A** to the Internet through the ZyXEL Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

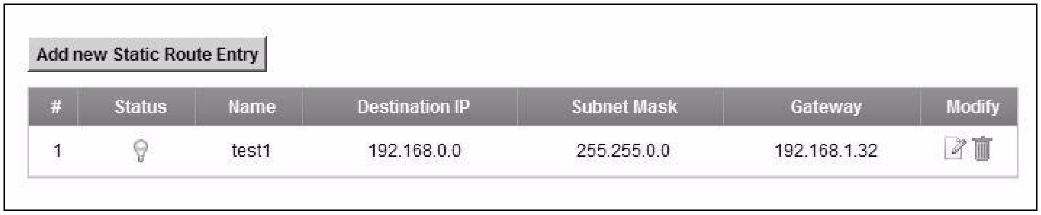
Figure 87 Example of Static Routing Topology



15.2 The Routing Screen

Use this screen to view and configure the static route rules on the ZyXEL Device. Click **Advanced > Routing** to open the following screen.

Figure 88 Advanced >Routing



Add new Static Route Entry

#	Status	Name	Destination IP	Subnet Mask	Gateway	Modify
1	💡	test1	192.168.0.0	255.255.0.0	192.168.1.32	📝🗑

The following table describes the labels in this screen.

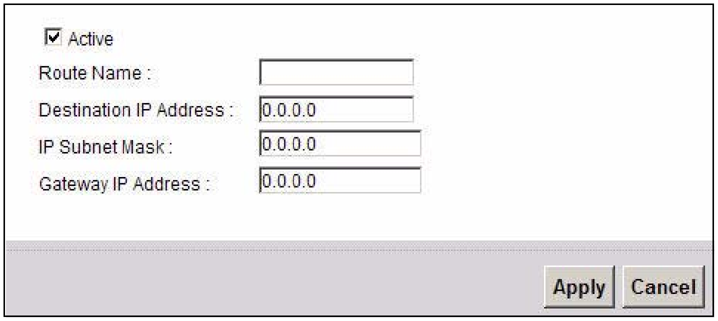
Table 65 Advanced > Routing

LABEL	DESCRIPTION
Add new Static Route Entry	Click this to configure a new static route.
#	This is the index number of the entry.
Status	This field displays whether the static route is active or not. A yellow bulb signifies that this route is active. A gray bulb signifies that this route is not active.
Name	This is the name that describes or identifies this route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Modify	Click the **Edit** icon to edit the static route on the ZyXEL Device. Click the **Delete** icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.

15.2.1 Add/Edit Static Route

Use this screen to add or edit a static route. Click **Add new Static Route Entry** in the **Routing** screen or the **Edit** icon next to the static route you want to edit. The screen shown next appears.

Figure 89 Routing: Add/Edit



☑ Active

Route Name :	
Destination IP Address :	0.0.0.0
IP Subnet Mask :	0.0.0.0
Gateway IP Address :	0.0.0.0

The following table describes the labels in this screen.

Table 66 Routing: Add/Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route. Select this to enable the static route. Clear this to disable this static route without having to delete the entry.
Route Name	Enter a descriptive name for the static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

16

Dynamic DNS Setup

16.1 Overview

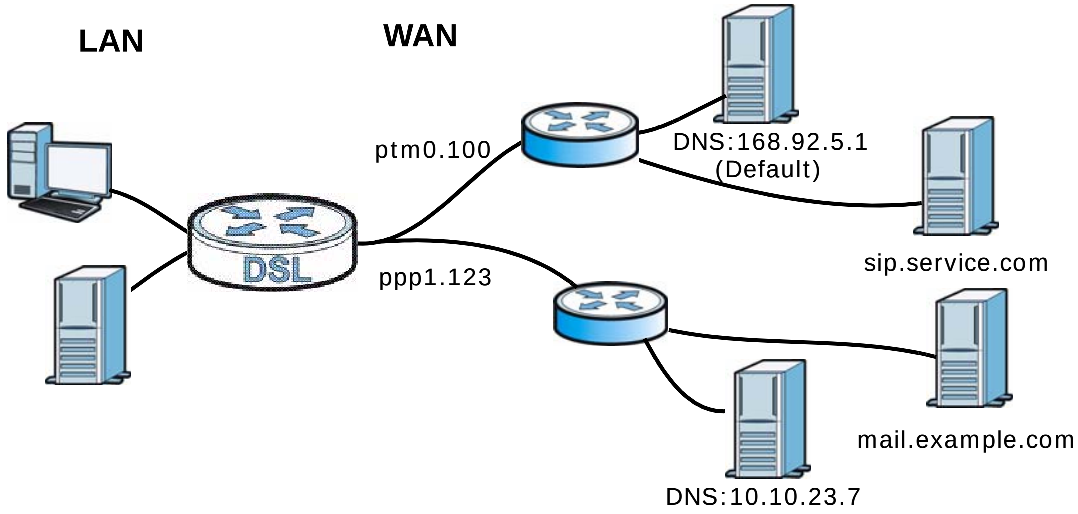
DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

In addition to the system DNS server(s), each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s). The ZyXEL Device uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the ZyXEL Device receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

In the following example, the DNS server 168.92.5.1 obtained from the WAN interface ptm0.100 is set to be the system DNS server. The DNS server 10.10.23.7 is obtained from the WAN interface ppp1.123. You configure a DNS route for *example.com to have the ZyXEL Device forward DNS requests for the domain name mail.example.com through the WAN interface ppp1.123 to the DNS server 10.10.23.7.

Figure 90 Example of DNS Routing Topology



Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

16.1.1 What You Can Do in this Chapter

- Use the **DNS Entry** screen to view, configure, or remove DNS routes (Section 16.2 on page 207).
- Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the ZyXEL Device (Section 16.3 on page 208).

16.1.2 What You Need To Know

DYNDNS Wildcard

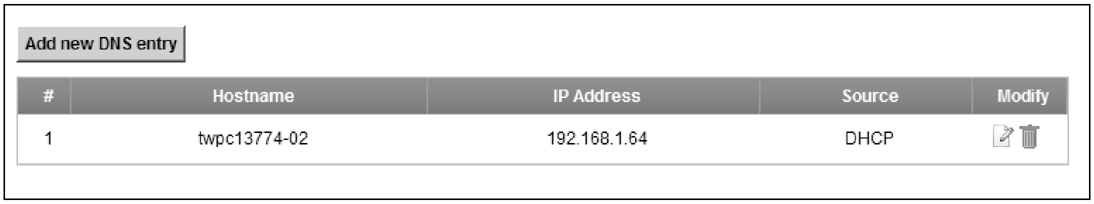
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

16.2 The DNS Entry Screen

Use this screen to view and configure DNS routes on the ZyXEL Device. Click **Advanced > DNS Setting** to open the **DNS Entry** screen.

Figure 91 Advanced > DNS Setting > DNS Setting



#	Hostname	IP Address	Source	Modify
1	twpc13774-02	192.168.1.64	DHCP	

The following table describes the fields in this screen.

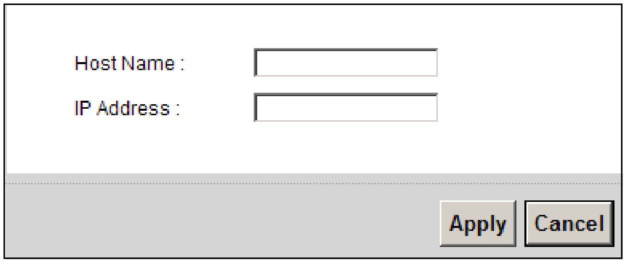
Table 67 Advanced > DNS Setting > DNS Setting

LABEL	DESCRIPTION
Add new DNS entry	Click this to create a new DNS entry.
#	This is the index number of the entry.
Hostname	This indicates the host name or domain name.
IP Address	This indicates the IP address assigned to this computer.
Source	This indicates the source of the IP address.
Modify	Click the **Edit** icon to edit the rule. Click the **Delete** icon to delete an existing rule.

16.2.1 Add/Edit DNS Entry

You can manually add or edit the ZyXEL Device’s DNS name and IP address entry. Click **Add new DNS entry** in the **DNS Entry** screen or the **Edit** icon next to the entry you want to edit. The screen shown next appears.

Figure 92 DNS Entry: Add/Edit



The following table describes the labels in this screen.

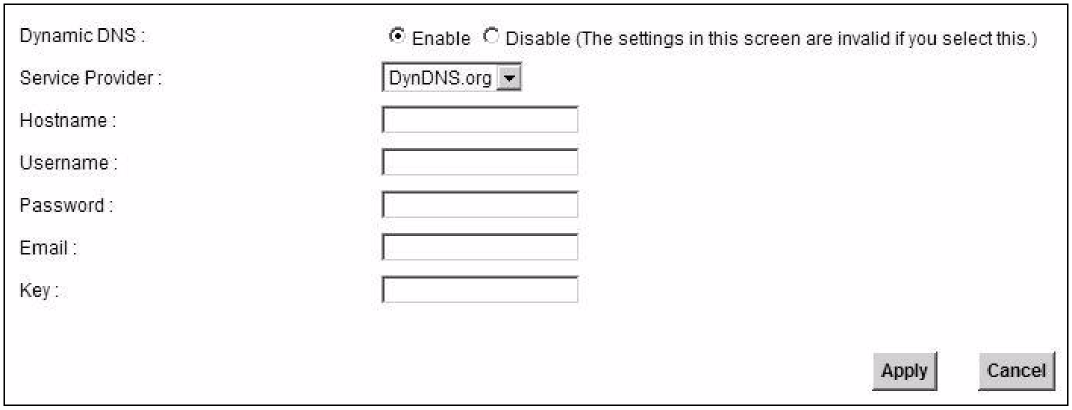
Table 68 DNS Entry: Add/Edit

LABEL	DESCRIPTION
Host Name	Enter the host name of the DNS entry.
IP Address	Enter the IP address of the DNS entry.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

16.3 The Dynamic DNS Screen

Use this screen to change your ZyXEL Device’s DDNS. Click **Advanced > DNS Setting > Dynamic DNS**. The screen appears as shown.

Figure 93 Advanced > DNS Setting > Dynamic DNS



Dynamic DNS : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

Service Provider : DynDNS.org

The following table describes the fields in this screen.

Table 69 Advanced > DNS Setting > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select your Dynamic DNS service provider from the drop-down list box.
Hostname	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Email	If you select **TZO** in the **Service Provider** field, enter the user name you used to register for this service.
Key	If you select **TZO** in the **Service Provider** field, enter the password you used to register for this service.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

17

Quality of Service (QoS)

17.1 Overview

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

Configure QoS on the ZyXEL Device to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves these steps:

1. Configure classifiers to sort traffic into different flows.
2. Assign priority and define actions to be performed for a classified traffic flow.

The ZyXEL Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

This chapter contains information about configuring QoS and editing classifiers.

17.1.1 What You Can Do in this Chapter

- The **General** screen lets you enable or disable QoS and set the upstream bandwidth (Section 17.3 on page 213).
- The **Queue Setup** screen lets you configure QoS queue assignment (Section 17.4 on page 214).
- The **Class Setup** screen lets you add, edit or delete QoS classifiers (Section 17.5 on page 216).
- The **Policer Setup** screen lets you add, edit or delete QoS policers (Section 17.5 on page 216).

- The **Monitor** screen lets you view the ZyXEL Device's QoS-related packet statistics (Section 17.7 on page 224).

17.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

QoS versus CoS

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

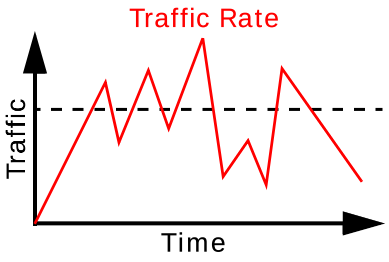
CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

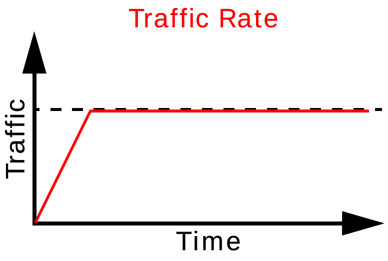
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Traffic Shaping

Bursty traffic may cause network congestion. Traffic shaping regulates packets to be transmitted with a pre-configured data transmission rate using buffers (or queues). Your ZyXEL Device uses the Token Bucket algorithm to allow a certain amount of large bursts while keeping a limit at the average rate.



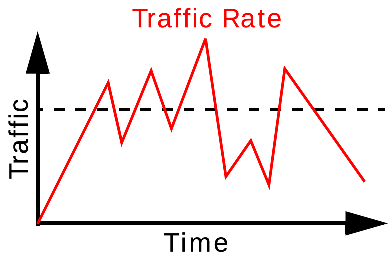
(Before Traffic Shaping)



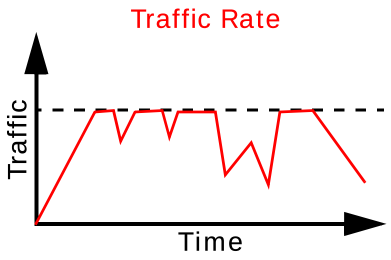
(After Traffic Shaping)

Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.



(Before Traffic Policing)



(After Traffic Policing)

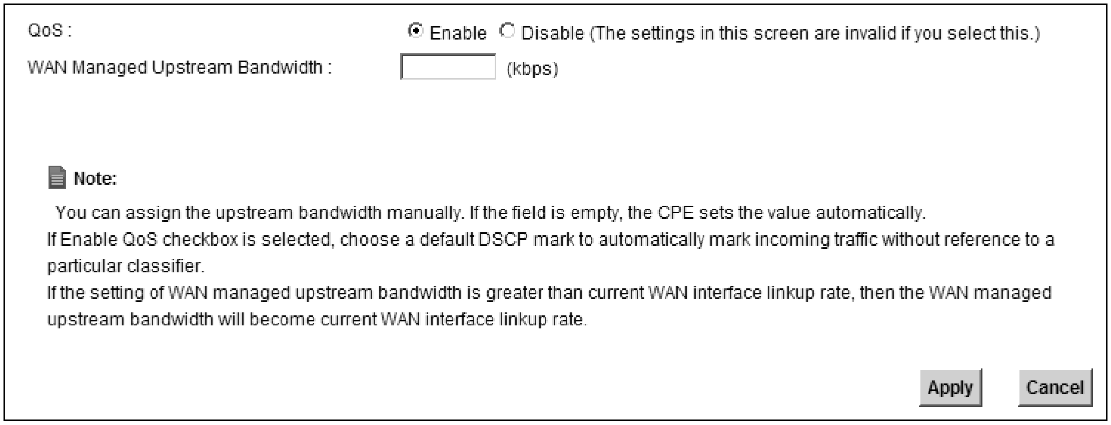
The ZyXEL Device supports three incoming traffic metering algorithms: Token Bucket Filter (TBF), Single Rate Two Color Maker (srTCM), and Two Rate Two Color Marker (trTCM). You can specify actions which are performed on the colored packets. See Section 17.8 on page 225 for more information on each metering algorithm.

17.3 The Quality of Service General Screen

Click **Advanced > QoS > General** to open the screen as shown next.

Use this screen to enable or disable QoS and set the upstream bandwidth. See Section 17.1 on page 211 for more information.

Figure 94 Advanced > QoS > General



QoS : ● Enable ○ Disable (The settings in this screen are invalid if you select this.)

WAN Managed Upstream Bandwidth : [ ] (kbps)

Note:

You can assign the upstream bandwidth manually. If the field is empty, the CPE sets the value automatically.
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier.
If the setting of WAN managed upstream bandwidth is greater than current WAN interface linkup rate, then the WAN managed upstream bandwidth will become current WAN interface linkup rate.

The following table describes the labels in this screen.

Table 70 Advanced > QoS > General

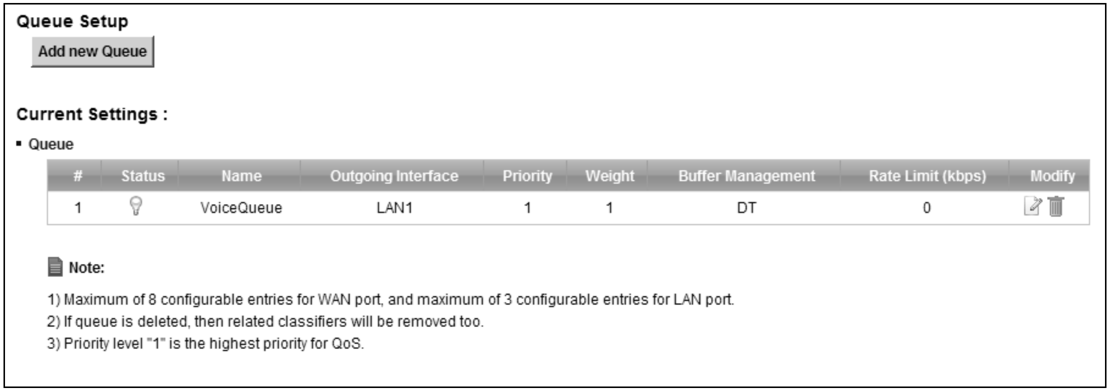
LABEL	DESCRIPTION
QoS	Select the **Enable** check box to turn on QoS to improve your network performance.
WAN Managed Upstream Bandwidth	Enter the amount of upstream bandwidth for the WAN interface that you want to allocate using QoS. The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can set this number higher than the interface's actual transmission speed. The ZyXEL Device uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed. You can also set this number lower than the interface's actual transmission speed. This will cause the ZyXEL Device to not use some of the interface's available bandwidth. If you leave this field blank, the ZyXEL Device automatically sets this number to be 95% of the DSL port's actual upstream transmission speed.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

17.4 The Queue Setup Screen

Click **Advanced > QoS > Queue Setup** to open the screen as shown next.

Use this screen to configure QoS queue assignment.

Figure 95 Advanced > QoS > Queue Setup



Current Settings :

- Queue

#	Status	Name	Outgoing Interface	Priority	Weight	Buffer Management	Rate Limit (kbps)	Modify
1		VoiceQueue	LAN1	1	1	DT	0	

Note:

1) Maximum of 8 configurable entries for WAN port, and maximum of 3 configurable entries for LAN port.
2) If queue is deleted, then related classifiers will be removed too.
3) Priority level "1" is the highest priority for QoS.

The following table describes the labels in this screen.

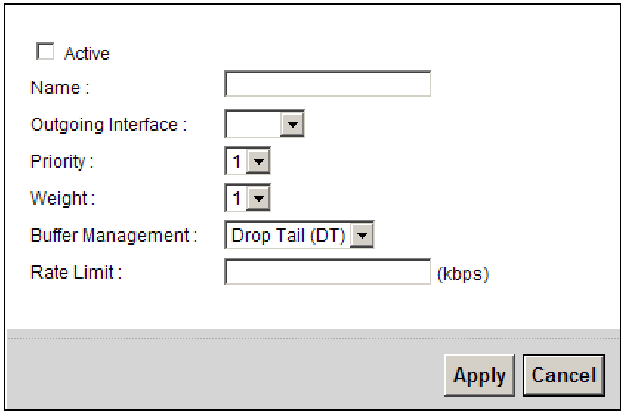
Table 71 Advanced > QoS > Queue Setup

LABEL	DESCRIPTION
Add new Queue	Click this button to create a new queue entry.
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Outgoing Interface	This shows the name of the ZyXEL Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used for this queue. Queue management algorithms determine how the ZyXEL Device should handle packets when it receives too many (network congestion).
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

17.4.1 Adding a QoS Queue

Click **Add new Queue** or the edit icon in the **Queue Setup** screen to configure a queue.

Figure 96 Queue Setup: Add



☐ Active

Name :

Outgoing Interface :

Priority : 1

Weight : 1

Buffer Management : Drop Tail (DT)

Rate Limit : (kbps)

The following table describes the labels in this screen.

Table 72 Queue Setup: Add

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Outgoing Interface	Select the interface to which this queue is applied. This field is read-only if you are editing the queue.
Priority	Select the priority level (from 1 to 3) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 8) of this queue. If two queues have the same priority level, the ZyXEL Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Buffer Management	This field displays **Drop Tail (DT)**. **Drop Tail (DT)** is a simple queue management algorithm that allows the ZyXEL Device buffer to accept as many packets as it can until it is full. Once the buffer is full, new packets that arrive are dropped until there is space in the buffer again (packets are transmitted out of it).
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

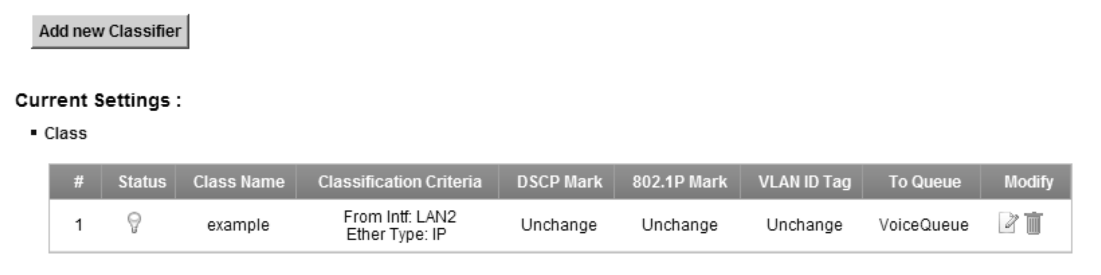
17.5 The Class Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Advanced > QoS > Class Setup** to open the following screen.

Figure 97 Advanced > QoS > Class Setup



#	Status	Class Name	Classification Criteria	DSCP Mark	802.1P Mark	VLAN ID Tag	To Queue	Modify
1		example	From Intf: LAN2 Ether Type: IP	Unchange	Unchange	Unchange	VoiceQueue	

The following table describes the labels in this screen.

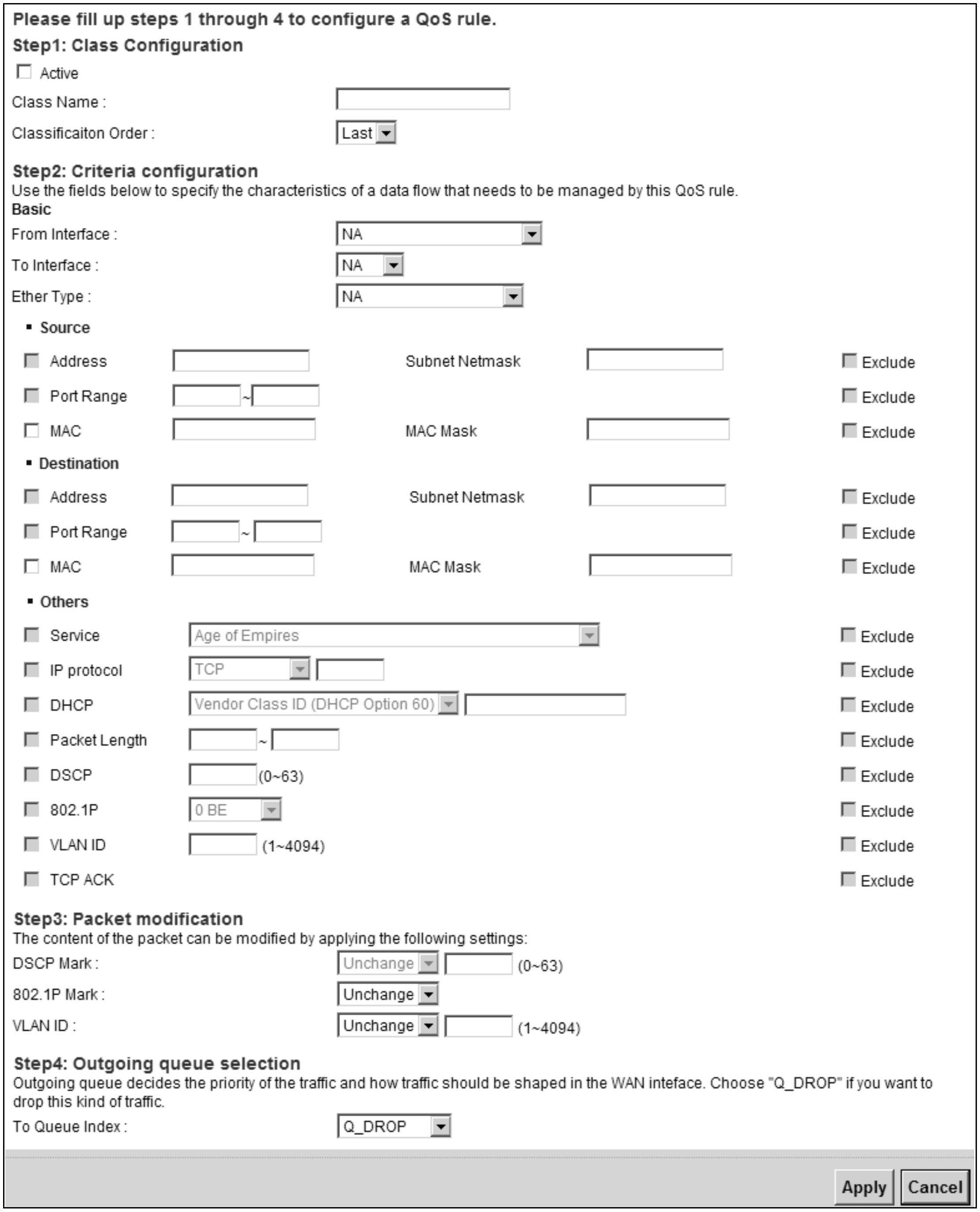
Table 73 Advanced > QoS > Class Setup

LABEL	DESCRIPTION
Add new Classifier	Click this to create a new classifier.
#	This is the index number of the entry.
Status	This field displays whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to edit the classifier. Click the **Delete** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

17.5.1 Add/Edit QoS Class

Click **Add new Classifier** in the **Class Setup** screen or the **Edit** icon next to a classifier to open the following screen.

Figure 98 Class Setup: Add/Edit



Please fill up steps 1 through 4 to configure a QoS rule.

Step1: Class Configuration

□ Active

Class Name :	
Classificaiton Order :	Last

Step2: Criteria configuration

Use the fields below to specify the characteristics of a data flow that needs to be managed by this QoS rule.

Basic

From Interface :	NA
To Interface :	NA
Ether Type :	NA

- **Source**

□ Address		Subnet Netmask		□ Exclude
□ Port Range	~			□ Exclude
□ MAC		MAC Mask		□ Exclude

- **Destination**

□ Address		Subnet Netmask		□ Exclude
□ Port Range	~			□ Exclude
□ MAC		MAC Mask		□ Exclude

- **Others**

□ Service	Age of Empires	□ Exclude
□ IP protocol	TCP	□ Exclude
□ DHCP	Vendor Class ID (DHCP Option 60)	□ Exclude
□ Packet Length	~	□ Exclude
□ DSCP	(0~63)	□ Exclude
□ 802.1P	0 BE	□ Exclude
□ VLAN ID	(1~4094)	□ Exclude
□ TCP ACK		□ Exclude

Step3: Packet modification

The content of the packet can be modified by applying the following settings:

DSCP Mark :	Unchange (0~63)
802.1P Mark :	Unchange
VLAN ID :	Unchange (1~4094)

Step4: Outgoing queue selection

Outgoing queue decides the priority of the traffic and how traffic should be shaped in the WAN inteface. Choose "Q_DROP" if you want to drop this kind of traffic.

To Queue Index :	Q_DROP

The following table describes the labels in this screen.

Table 74 Class Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select this to enable this classifier.
Class Name	Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.
From Interface	If you want to classify the traffic by an ingress interface, select an interface from the **From Interface** drop-down list box.
To Interface	If you want to classify the traffic by an egress interface, select an interface from the **To Interface** drop-down list box.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select **802.1Q**, you can configure an 802.1p priority level.
Source	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet’s MAC address should match. Enter “f” for each bit of the specified source MAC address that the traffic’s MAC address should match. Enter “0“ for the bit(s) of the matched traffic’s MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
Subnet Netmask	Enter the source subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
MAC	Select the check box and enter the source MAC address of the packet.

Table 74 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
Service	This field is available only when you select **IP** in the **Ether Type** field. This field simplifies classifier configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the filter fields.
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select the protocol (service type) from **TCP**, **UDP**, **ICMP** or **IGMP**. If you select **User defined**, enter the protocol (service type) number.
DHCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select a DHCP option. If you select **Vendor Class ID (DHCP Option 60)**, enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware. If you select **User Class ID (DHCP Option 77)**, enter a string that identifies the user's category or application type in the matched DHCP packets.
Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1500) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
802.1P	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and select a priority level (between 0 and 7) from the drop-down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and specify a VLAN ID number.

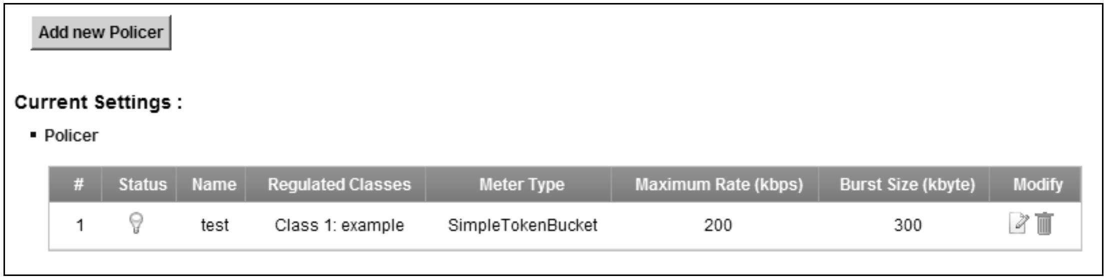
Table 74 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
DSCP Mark	This field is available only when you select **IP** in the **Ether Type** field. If you select **Mark**, enter a DSCP value with which the ZyXEL Device replaces the DSCP field in the packets. If you select **Unchange**, the ZyXEL Device keep the DSCP field in the packets.
802.1P Mark	Select a priority level with which the ZyXEL Device replaces the IEEE 802.1p priority field in the packets. If you select **Unchange**, the ZyXEL Device keep the 802.1p priority field in the packets.
VLAN ID	If you select **Remark**, enter a VLAN ID number with which the ZyXEL Device replaces the VLAN ID of the frames. If you select **Remove**, the ZyXEL Device deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the ZyXEL Device treat all matched traffic untagged and add a second VLAN ID. If you select **Unchange**, the ZyXEL Device keep the VLAN ID in the packets.
To Queue Index	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

17.6 The QoS Policer Setup Screen

Use this screen to configure QoS policers that allow you to limit the transmission rate of incoming traffic. Click **Advanced > QoS > Policer Setup**. The screen appears as shown.

Figure 99 Advanced > QoS > Policer Setup



Current Settings :

- Policer

#	Status	Name	Regulated Classes	Meter Type	Maximum Rate (kbps)	Burst Size (kbyte)	Modify
1	💡	test	Class 1: example	SimpleTokenBucket	200	300	✎ 🗑

The following table describes the labels in this screen.

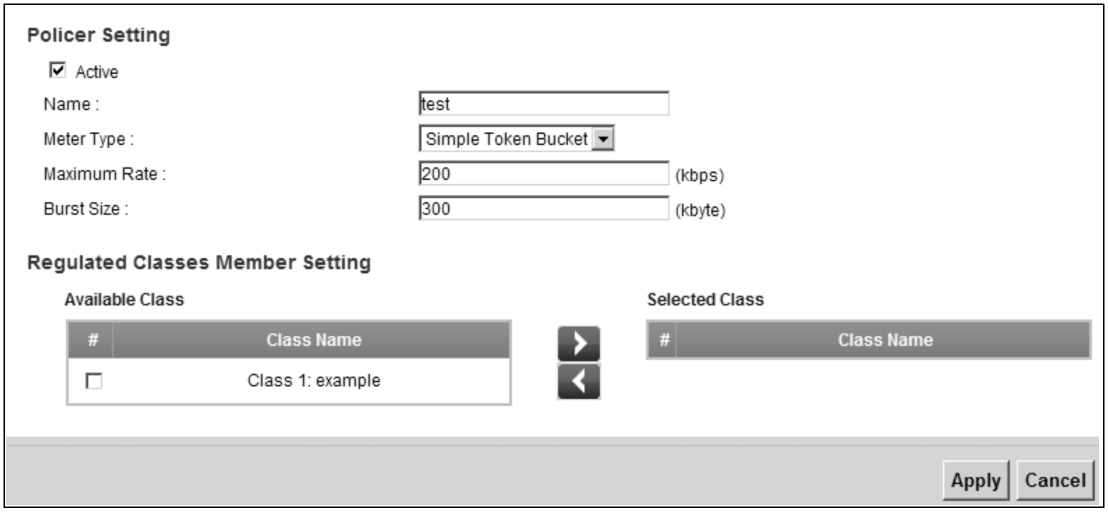
Table 75 Advanced > QoS > Policer Setup

LABEL	DESCRIPTION
Add new Policer	Click this to create a new entry.
#	This is the index number of the entry.
Status	This field displays whether the policer is active or not. A yellow bulb signifies that this policer is active. A gray bulb signifies that this policer is not active.
Name	This field displays the descriptive name of this policer.
Regulated Classes	This field displays the name of a QoS classifier
Meter Type	This field displays the type of QoS metering algorithm used in this policer.
Maximum Rate	This field displays the maximum rate configured for the metering algorithm in the policer.
Burst Size	This field displays the burst size configured for the metering algorithm in the policer.
Modify	Click the **Edit** icon to edit the policer. Click the **Delete** icon to delete an existing policer. Note that subsequent rules move up by one when you take this action.

17.6.1 Add/Edit a QoS Policer

Click **Add new Officer** in the **Policer Setup** screen or the **Edit** icon next to a policer to show the following screen.

Figure 100 Policer Setup: Add/Edit



Policer Setting

☑ Active

Name : test

Meter Type : Simple Token Bucket

Maximum Rate : 200 (kbps)

Burst Size : 300 (kbyte)

Regulated Classes Member Setting

Available Class

#	Class Name
□	Class 1: example

Selected Class

#	Class Name

The following table describes the labels in this screen.

Table 76 Policer Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select the check box to activate this policer.
Name	Enter the descriptive name of this policer.
Meter Type	This shows the traffic metering algorithm used in this policer. The **Simple Token Bucket** algorithm uses tokens in a bucket to control when traffic can be transmitted. Each token represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size.
Maximum Rate	Specify the guaranteed rate at which packets are admitted to the network. This is to specify how many bytes of tokens are added to a bucket every second.
Burst Size	Specify the guaranteed amount of bytes that are admitted at the committed rate. This is the maximum size of the (first) token bucket in a traffic metering algorithm.
Available Class Selected Class	Select a QoS classifier to apply this QoS policer to traffic that matches the QoS classifier. Highlight a QoS classifier in the **Available Class** box and use the **>** button to move it to the **Selected Class** box. To remove a QoS classifier from the **Selected Class** box, select it and use the **<** button.

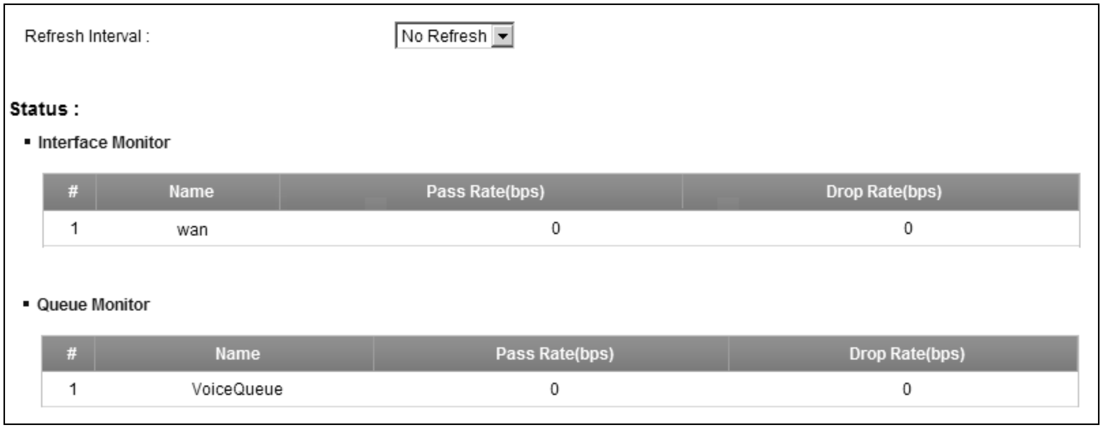
Table 76 Policer Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

17.7 The QoS Monitor Screen

To view the ZyXEL Device's QoS packet statistics, click **Advanced > QoS > Monitor**. The screen appears as shown.

Figure 101 Advanced > QoS > Monitor



Refresh Interval : No Refresh

Status :

- **Interface Monitor**

#	Name	Pass Rate(bps)	Drop Rate(bps)
1	wan	0	0

- **Queue Monitor**

#	Name	Pass Rate(bps)	Drop Rate(bps)
1	VoiceQueue	0	0

The following table describes the labels in this screen.

Table 77 Advanced > QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the ZyXEL Device to update this screen. Select **No Refresh** to stop refreshing statistics.
Interface Monitor	
#	This is the index number of the entry.
Name	This shows the name of the WAN interface on the ZyXEL Device.
Pass Rate	This shows how many packets forwarded to this interface are transmitted successfully.
Drop Rate	This shows how many packets forwarded to this interface are dropped.
Queue Monitor	
#	This is the index number of the entry.
Name	This shows the name of the queue.
Pass Rate	This shows how many packets assigned to this queue are transmitted successfully.
Drop Rate	This shows how many packets assigned to this queue are dropped.

17.8 Technical Reference

The following section contains additional technical information about the ZyXEL Device features described in this chapter.

IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 78 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new Differentiated Services (DS) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

Automatic Priority Queue Assignment

If you enable QoS on the ZyXEL Device, the ZyXEL Device can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the ZyXEL Device. On the ZyXEL Device, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 79 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000 111000	
		7		

Token Bucket

The token bucket algorithm uses tokens in a bucket to control when traffic can be transmitted. The bucket stores tokens, each of which represents one byte. The algorithm allows bursts of up to *b* bytes which is also the bucket size, so the bucket can hold up to *b* tokens. Tokens are generated and added into the bucket at a constant rate. The following shows how tokens work with packets:

- A packet can be transmitted if the number of tokens in the bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the bucket.
- If there are no tokens in the bucket, the ZyXEL Device stops transmitting until enough tokens are generated.
- If not enough tokens are available, the ZyXEL Device treats the packet in either one of the following ways:

  In traffic shaping:

  - Holds it in the queue until enough tokens are available in the bucket.

  In traffic policing:

  - Drops it.
  - Transmits it but adds a DSCP mark. The ZyXEL Device may drop these marked packets if the network is overloaded.

Configure the bucket size to be equal to or less than the amount of the bandwidth that the interface can support. It does not help if you set it to a bucket size over the interface’s capability. The smaller the bucket size, the lower the data transmission rate and that may cause outgoing packets to be dropped. A larger transmission rate requires a big bucket size. For example, use a bucket size of 10 kbytes to get the transmission rate up to 10 Mbps.

Single Rate Three Color Marker

The Single Rate Three Color Marker (srTCM, defined in RFC 2697) is a type of traffic policing that identifies packets by comparing them to one user-defined rate, the Committed Information Rate (CIR), and two burst sizes: the Committed Burst Size (CBS) and Excess Burst Size (EBS).

The srTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The srTCM is based on the token bucket filter and has two token buckets (CBS and EBS). Tokens are generated and added into the bucket at a constant rate, called Committed Information Rate (CIR). When the first bucket (CBS) is full, new tokens overflow into the second bucket (EBS).

All packets are evaluated against the CBS. If a packet does not exceed the CBS it is marked green. Otherwise it is evaluated against the EBS. If it is below the EBS then it is marked yellow. If it exceeds the EBS then it is marked red.

The following shows how tokens work with incoming packets in srTCM:

- A packet arrives. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes).
- After a packet is transmitted, a number of tokens corresponding to the packet size is removed from the CBS bucket.
- If there are not enough tokens in the CBS bucket, the ZyXEL Device checks the EBS bucket. The packet is marked yellow if there are sufficient tokens in the EBS bucket. Otherwise, the packet is marked red. No tokens are removed if the packet is dropped.

Two Rate Three Color Marker

The Two Rate Three Color Marker (trTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

The trTCM evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green.

The trTCM is based on the token bucket filter and has two token buckets (Committed Burst Size (CBS) and Peak Burst Size (PBS)). Tokens are generated and added into the two buckets at the CIR and PIR respectively.

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

The following shows how tokens work with incoming packets in trTCM:

- A packet arrives. If the number of tokens in the PBS bucket is less than the size of the packet (in bytes), the packet is marked red and may be dropped regardless of the CBS bucket. No tokens are removed if the packet is dropped.
- If the PBS bucket has enough tokens, the ZyXEL Device checks the CBS bucket. The packet is marked green and can be transmitted if the number of tokens in the CBS bucket is equal to or greater than the size of the packet (in bytes). Otherwise, the packet is marked yellow.

18

TR-069 Client

18.1 Overview

This chapter explains how to configure the ZyXEL Device’s TR-069 auto-configuration settings

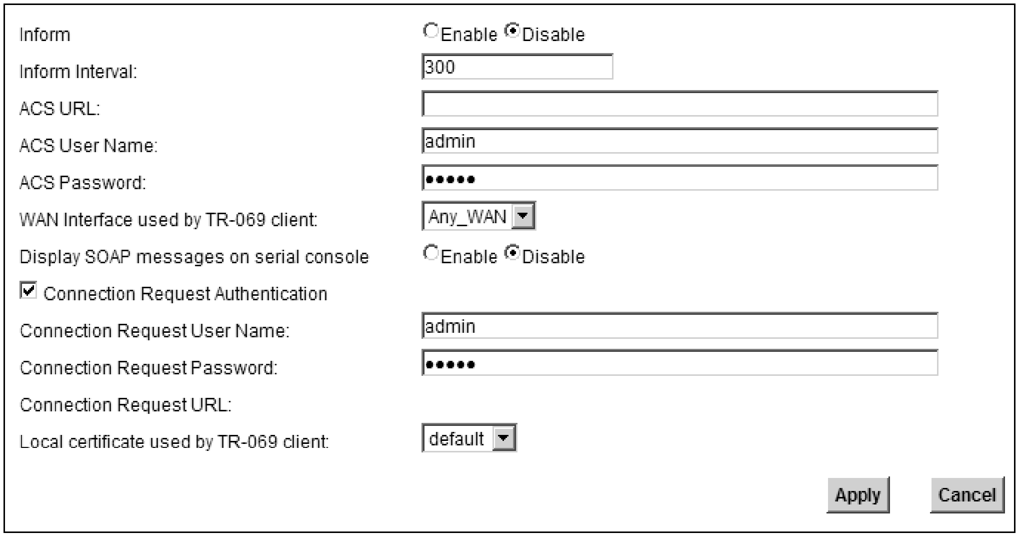
18.2 The TR-069 Clients Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your ZyXEL Device, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the ZyXEL Device, modify settings, perform firmware upgrades as well as monitor and diagnose the ZyXEL Device. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Advanced > TR-069 Clients** to open the following screen. Use this screen to configure your ZyXEL Device to be managed by an ACS.

Figure 102 Advanced > TR-069 Clients



Inform	○ Enable ● Disable
Inform Interval:	300
ACS URL:	
ACS User Name:	admin
ACS Password:	•••••
WAN Interface used by TR-069 client:	Any_WAN
Display SOAP messages on serial console	○ Enable ● Disable
☑ Connection Request Authentication	
Connection Request User Name:	admin
Connection Request Password:	•••••
Connection Request URL:	
Local certificate used by TR-069 client:	default

The following table describes the fields in this screen.

Table 80 Advanced > TR-069 Clients

LABEL	DESCRIPTION
Inform	Select **Enable** for the ZyXEL Device to send periodic inform via TR-069 on the WAN. Otherwise, select **Disable**.
Inform Interval	Enter the time interval (in seconds) at which the ZyXEL Device sends information to the auto-configuration server.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	Select a WAN interface through which the TR-069 traffic passes. If you select **Any_WAN**, you should also select the pre-configured WAN connection(s).
Display SOAP messages on serial console	Select **Enable** to show the SOAP messages on the console.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the ZyXEL Device, this user name is used to authenticate the ACS.

Table 80 Advanced > TR-069 Clients (continued)

LABEL	DESCRIPTION
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the ZyXEL Device, this password is used to authenticate the ACS.
Connection Request URL	This shows the connection request URL. The ACS can use this URL to make a connection request to the ZyXEL Device.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

19

Time Settings

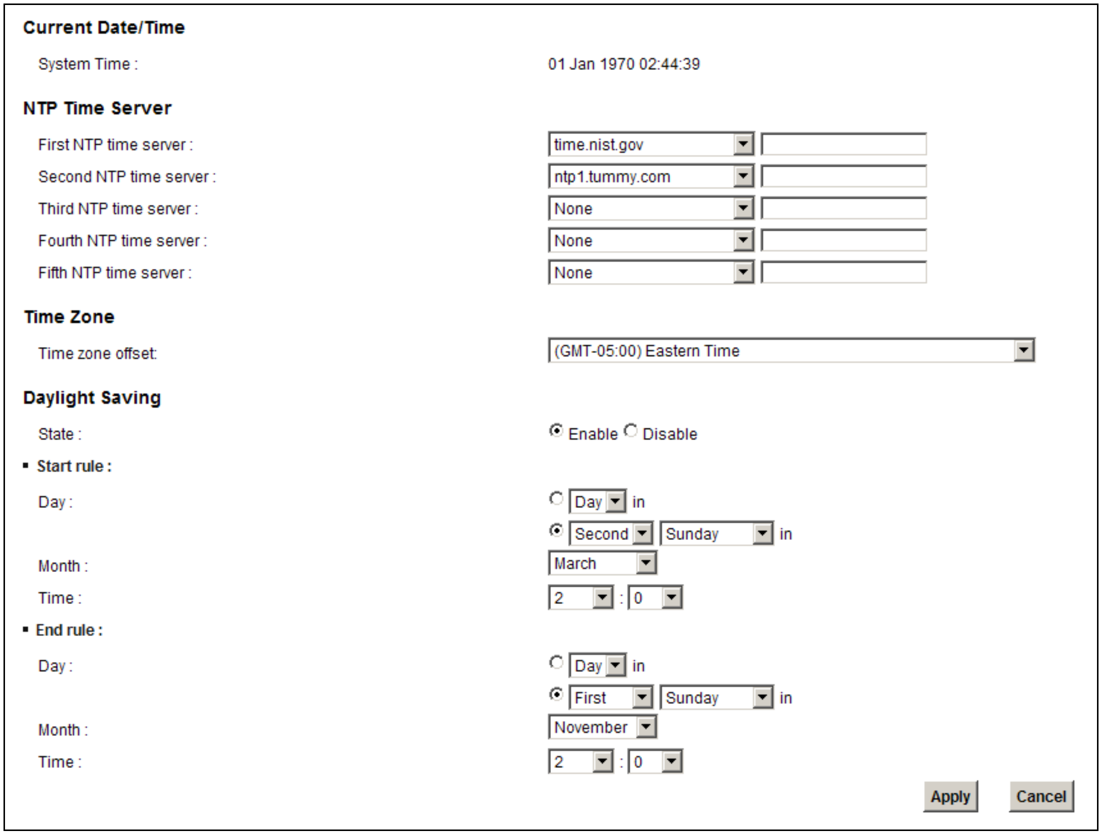
19.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

19.2 The Time Setting Screen

To change your ZyXEL Device's time and date, click **Advanced >Time Setting**. The screen appears as shown. Use this screen to configure the ZyXEL Device's time based on your local time zone.

Figure 103 Advanced >Time Setting



Current Date/Time

System Time :	01 Jan 1970 02:44:39

NTP Time Server

First NTP time server :	time.nist.gov	
Second NTP time server :	ntp1.tummy.com	
Third NTP time server :	None	
Fourth NTP time server :	None	
Fifth NTP time server :	None	

Time Zone

Time zone offset:	(GMT-05:00) Eastern Time

Daylight Saving

State :	● Enable ○ Disable
▪ **Start rule :**	
Day :	○ Day in ● Second Sunday in
Month :	March
Time :	2 : 0
▪ **End rule :**	
Day :	○ Day in ● First Sunday in
Month :	November
Time :	2 : 0

The following table describes the fields in this screen.

Table 81 Advanced >Time Setting

LABEL	DESCRIPTION
Current Date/Time	
System Time	This field displays the time and fate of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the time and date with the time server.
NTP Time Server	
First ~ Fifth NTP time server	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select **None** if you don't want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	
Time zone offset	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	
State	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.Select **Enable** if you use Daylight Saving Time.
Start rule	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type **2** in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 81 Advanced >Time Setting (continued)

LABEL	DESCRIPTION
End rule	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type **2** in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

Scheduler Rules

20.1 Overview

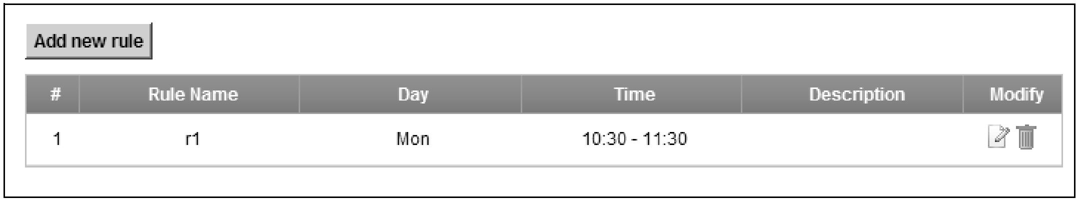
You can define time periods and days during which the ZyXEL Device performs scheduled rules of certain features (such as Firewall Access Control, Parental Control) on a specific user in the **Scheduler Rules** screen.

20.2 The Scheduler Rules Screen

Use this screen to view, add, or edit time schedule rules.

Click **Advanced > Scheduler Rules** to open the following screen.

Figure 104 Advanced > Scheduler Rules



#	Rule Name	Day	Time	Description	Modify
1	r1	Mon	10:30 - 11:30		

The following table describes the fields in this screen.

Table 82 Advanced > Scheduler Rules

LABEL	DESCRIPTION
Add new rule	Click this to create a new rule.
#	This is the index number of the entry.
Rule Name	This shows the name of the rule.
Day	This shows the day(s) on which this rule is enabled.
Time	This shows the period of time on which this rule is enabled.

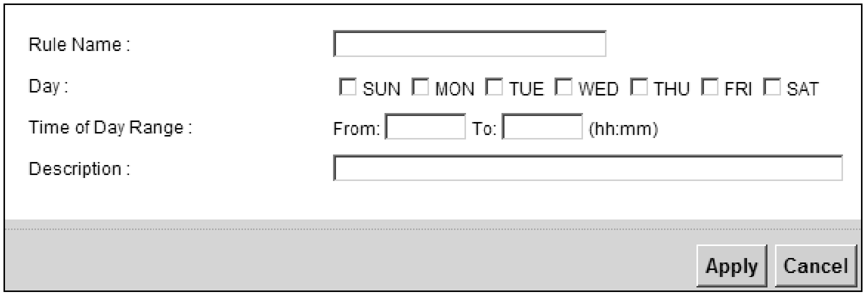
Table 82 Advanced > Scheduler Rules (continued)

LABEL	DESCRIPTION
Description	This shows the description of this rule.
Modify	Click the **Edit** icon to edit the schedule. Click the **Delete** icon to delete a scheduler rule. Note: You cannot delete a scheduler rule once it is applied to a certain feature.

20.2.1 Add/Edit a Schedule

Click the **Add** button in the **Scheduler Rules** screen or click the **Edit** icon next to a schedule rule to open the following screen. Use this screen to configure a restricted access schedule for a specific user on your network.

Figure 105 Scheduler Rules: Add/Edit



Rule Name :

Day : □ SUN □ MON □ TUE □ WED □ THU □ FRI □ SAT

Time of Day Range : From: To: (hh:mm)

Description :

The following table describes the fields in this screen.

Table 83 Scheduler Rules: Add/Edit

LABEL	DESCRIPTION
Rule Name	Enter a name (up to 31 printable English keyboard characters, not including spaces) for this schedule.
Day	Select check boxes for the days that you want the ZyXEL Device to perform this scheduler rule.
Time if Day Range	Enter the time period of each day, in 24-hour format, during which parental control will be enforced.
Description	Enter a description for this scheduler rule.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

21

Policy Forwarding

21.1 Overview

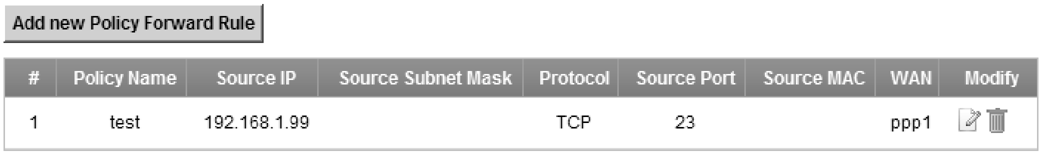
Traditionally, routing is based on the destination address only and the ZyXEL Device takes the shortest path to forward a packet. Policy forwarding allows the ZyXEL Device to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

You can use source-based policy forwarding to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

21.2 The Policy Forwarding Screen

The **Policy Forwarding** screens let you view and configure routing policies on the ZyXEL Device. Click **Advanced > Policy Forwarding** to open the **Policy Forwarding** screen.

Figure 106 Advanced > Policy Forwarding



#	Policy Name	Source IP	Source Subnet Mask	Protocol	Source Port	Source MAC	WAN	Modify
1	test	192.168.1.99		TCP	23		ppp1	✎ 🗑

The following table describes the labels in this screen.

Table 84 Advanced > Policy Forwarding

LABEL	DESCRIPTION
Add new Policy Forward Rule	Click this to create a new policy forwarding rule.
#	This is the index number of the entry.
Policy Name	This is the name of the rule.

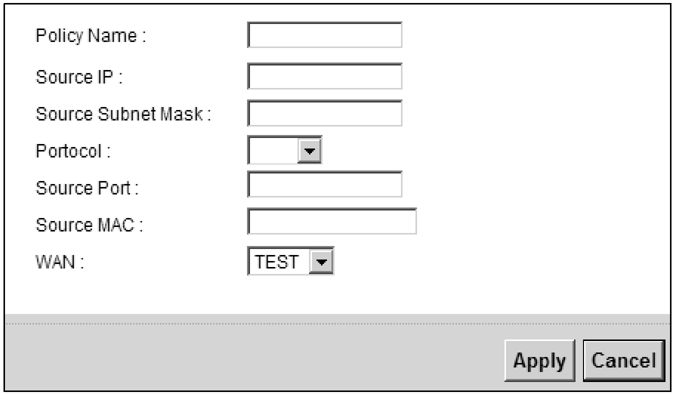
Table 84 Advanced > Policy Forwarding (continued)

LABEL	DESCRIPTION
Source IP	This is the source IP address.
Source Subnet Mask	This is the source subnet mask address.
Protocol	This is the transport layer protocol.
SourcePort	This is the source port number.
Source MAC	This is the source MAC address.
WAN	This is the WAN interface through which the traffic is routed.
Modify	Click the **Edit** icon to edit this policy. Click the **Delete** icon to delete an existing policy.

21.2.1 Add/Edit Policy Forwarding

Click **Add new Policy Forward Rule** in the **Policy Forwarding** screen or click the **Edit** icon next to a policy. Use this screen to configure the required information for a policy route.

Figure 107 Policy Forwarding: Add/Edit



Policy Name :

Source IP :

Source Subnet Mask :

Portocol :

Source Port :

Source MAC :

WAN : TEST

The following table describes the labels in this screen.

Table 85 Policy Forwarding: Add/Edit

LABEL	DESCRIPTION
Policy Name	Enter a descriptive name of up to 8 printable English keyboard characters, not including spaces.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask address.
Protocol	Select the transport layer protocol (**TCP** or **UDP**).
Source Port	Enter the source port number.
Source Mac	Enter the source MAC address.

Table 85 Policy Forwarding: Add/Edit (continued)

LABEL	DESCRIPTION
WAN	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **Broadband** screens.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

22

Logs

22.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the ZyXEL Device log and then display the logs or have the ZyXEL Device send them to an administrator (as e-mail) or to a syslog server.

22.1.1 What You Can Do in this Chapter

- Use the **System Log** screen to see the system logs for the categories that you select (Section 22.2 on page 246).
- Use the **Security Log** screen to see the security-related logs for the categories that you select (Section 22.3 on page 248).

22.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server.

Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

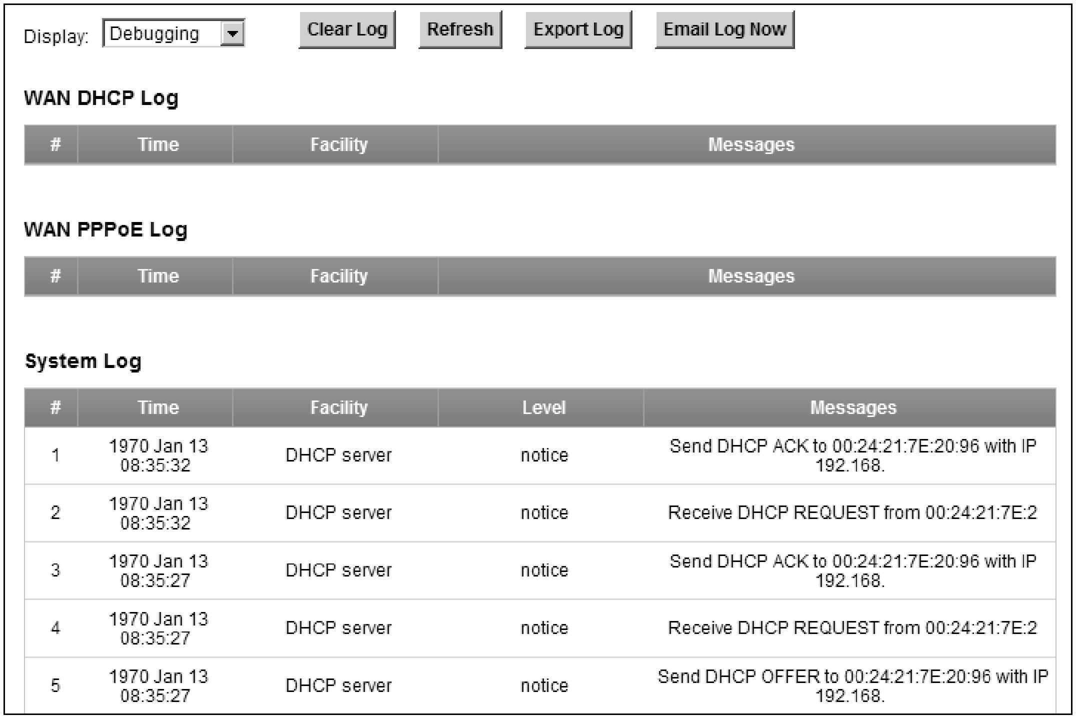
Table 86 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

22.2 The System Log Screen

Use the **System Log** screen to see the system logs for the categories that you select. Click **System Monitor > Log** to open the **System Log** screen.

Figure 108 System Monitor > Log > System Log



Display: Debugging

WAN DHCP Log

#	Time	Facility	Messages

WAN PPPoE Log

#	Time	Facility	Messages

System Log

#	Time	Facility	Level	Messages
1	1970 Jan 13 08:35:32	DHCP server	notice	Send DHCP ACK to 00:24:21:7E:20:96 with IP 192.168.
2	1970 Jan 13 08:35:32	DHCP server	notice	Receive DHCP REQUEST from 00:24:21:7E:2
3	1970 Jan 13 08:35:27	DHCP server	notice	Send DHCP ACK to 00:24:21:7E:20:96 with IP 192.168.
4	1970 Jan 13 08:35:27	DHCP server	notice	Receive DHCP REQUEST from 00:24:21:7E:2
5	1970 Jan 13 08:35:27	DHCP server	notice	Send DHCP OFFER to 00:24:21:7E:20:96 with IP 192.168.

The following table describes the fields in this screen.

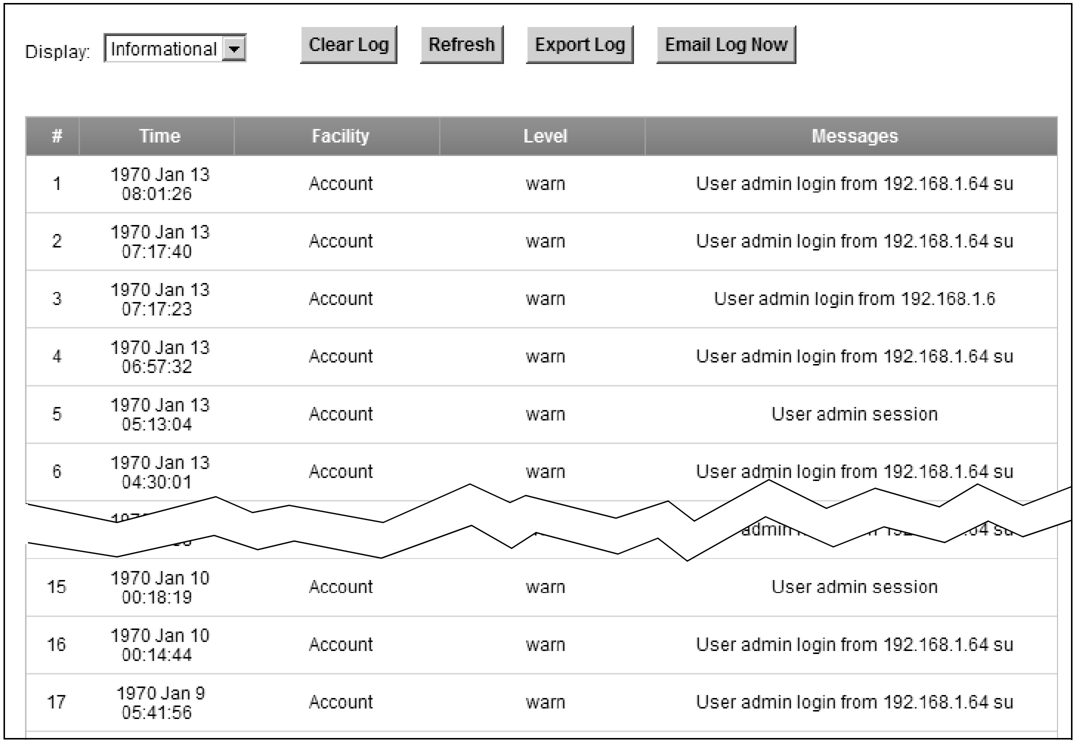
Table 87 System Monitor > Log > System Log

LABEL	DESCRIPTION
Display	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the ZyXEL Device searches through all logs of that severity or higher.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s).
Email Log Now	Click this to send the log file(s) to the E-mail address you specify in the **Maintenance > Logs Setting** screen.
WAN DHCP Log	
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Messages	This field states the reason for the log.
WAN PPPoE Log	
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Messages	This field states the reason for the log.
System Log	
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Messages	This field states the reason for the log.

22.3 The Security Log Screen

Use the **Security Log** screen to see the security-related logs for the categories that you select. Click **System Monitor > Log > Security Log** to open the following screen.

Figure 109 System Monitor > Log > Security Log



#	Time	Facility	Level	Messages
1	1970 Jan 13 08:01:26	Account	warn	User admin login from 192.168.1.64 su
2	1970 Jan 13 07:17:40	Account	warn	User admin login from 192.168.1.64 su
3	1970 Jan 13 07:17:23	Account	warn	User admin login from 192.168.1.6
4	1970 Jan 13 06:57:32	Account	warn	User admin login from 192.168.1.64 su
5	1970 Jan 13 05:13:04	Account	warn	User admin session
6	1970 Jan 13 04:30:01	Account	warn	User admin login from 192.168.1.64 su
15	1970 Jan 10 00:18:19	Account	warn	User admin session
16	1970 Jan 10 00:14:44	Account	warn	User admin login from 192.168.1.64 su
17	1970 Jan 9 05:41:56	Account	warn	User admin login from 192.168.1.64 su

The following table describes the fields in this screen.

Table 88 System Monitor > Log > Security Log

LABEL	DESCRIPTION
Display	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the ZyXEL Device searches through all logs of that severity or higher.
Clear Log	Click this to delete all the logs.
Refresh	Click this to renew the log screen.
Export Log	Click this to export the selected log(s).
Email Log Now	Click this to send the log file(s) to the E-mail address you specify in the **Maintenance > Logs Setting** screen.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.

Table 88 System Monitor > Log > Security Log (continued)

LABEL	DESCRIPTION
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Messages	This field states the reason for the log.

23

Introduction to the ARP Table

23.1 Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

23.1.1 How ARP Works

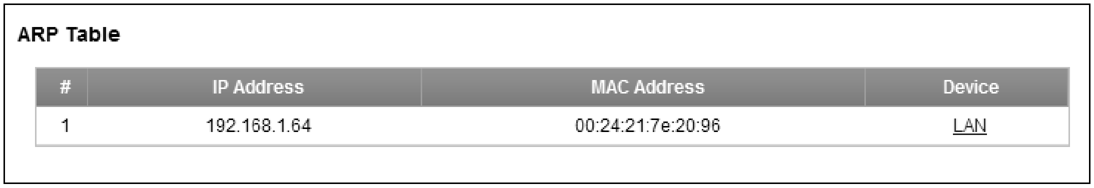
When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

23.2 ARP Table Screen

Use the ARP table to view IP-to-MAC address mapping(s). To open this screen, click **System Monitor** > **ARP Table**.

Figure 110 System Monitor > ARP Table



ARP Table

#	IP Address	MAC Address	Device
1	192.168.1.64	00:24:21:7e:20:96	LAN

The following table describes the labels in this screen.

Table 89 System Monitor > ARP Table

LABEL	DESCRIPTION
#	This is the ARP table entry number.
IP Address	This is the learned IP address of a device connected to a port.
MAC Address	This is the MAC address of the device with the listed IP address.
Device	This is the type of interface used by the device. You can click on the device type to go to its configuration screen.

24

Traffic Status

24.1 Overview

Use the **Traffic Status** screens to look at network traffic status and statistics of the WAN and LAN interfaces.

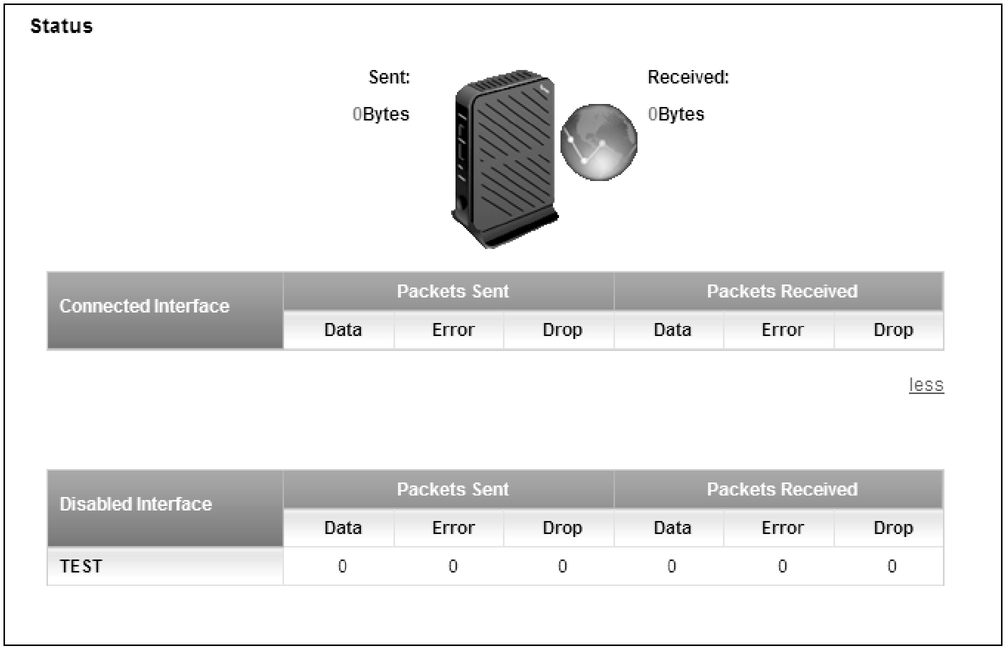
24.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 24.2 on page 254).
- Use the **LAN** screen to view the LAN traffic statistics (Section 24.3 on page 255).

24.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. The figure in this screen shows the number of bytes received and sent on the ZyXEL Device.

Figure 111 System Monitor > Traffic Status > WAN



Status

Sent:
0Bytes

Received:
0Bytes

Connected Interface	Packets Sent			Packets Received		
	Data	Error	Drop	Data	Error	Drop

less

Disabled Interface	Packets Sent			Packets Received		
	Data	Error	Drop	Data	Error	Drop
TEST	0	0	0	0	0	0

The following table describes the fields in this screen.

Table 90 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.
more.../less	Click **more...** to show more information. Click **less** to hide them.
Disabled Interface	This shows the name of the WAN interface that is currently disconnected.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.

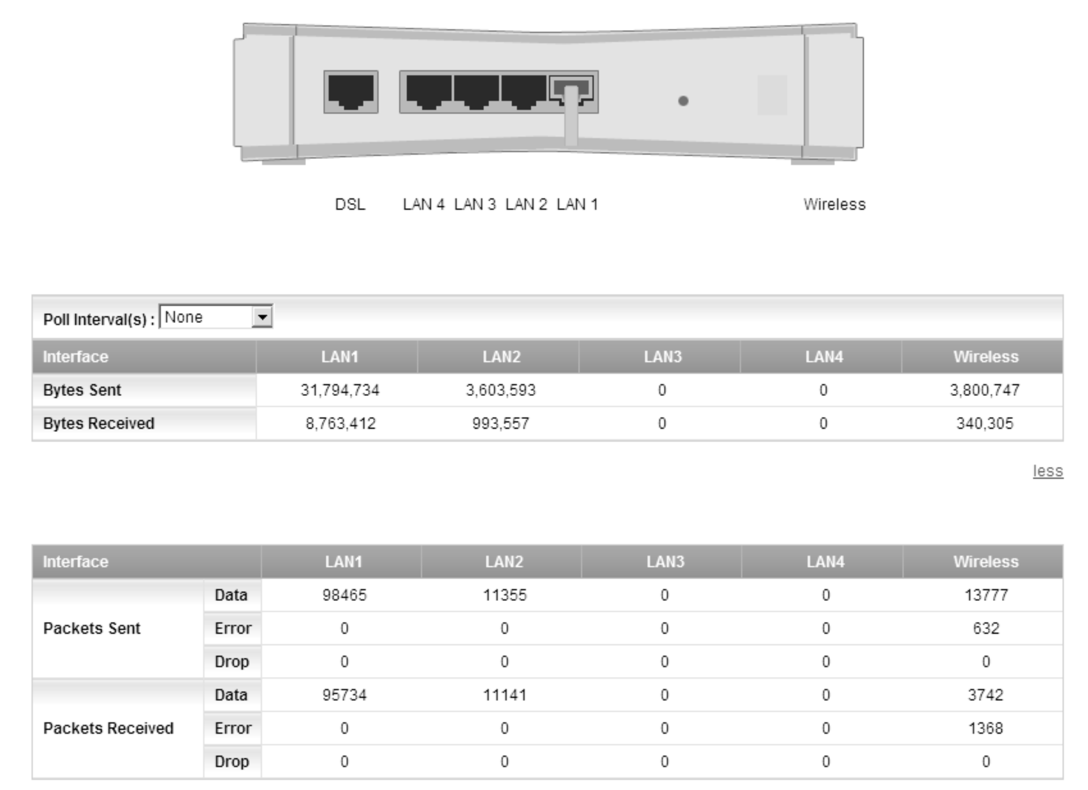
Table 90 System Monitor > Traffic Status > WAN (continued)

LABEL	DESCRIPTION
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

24.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. The figure in this screen shows the interface that is currently connected on the ZyXEL Device.

Figure 112 System Monitor > Traffic Status > LAN



Poll Interval(s) : None

Interface	LAN1	LAN2	LAN3	LAN4	Wireless
Bytes Sent	31,794,734	3,603,593	0	0	3,800,747
Bytes Received	8,763,412	993,557	0	0	340,305

Interface		LAN1	LAN2	LAN3	LAN4	Wireless
Packets Sent	Data	98465	11355	0	0	13777
	Error	0	0	0	0	632
	Drop	0	0	0	0	0
Packets Received	Data	95734	11141	0	0	3742
	Error	0	0	0	0	1368
	Drop	0	0	0	0	0

The following table describes the fields in this screen.

Table 91 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Polls Interval(s)	Select how often you want the ZyXEL Device to update this screen.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
more.../less	Click **more...** to show more information. Click **less** to hide them.
Interface	This shows the LAN or WLAN interface.
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

25

Users Configuration

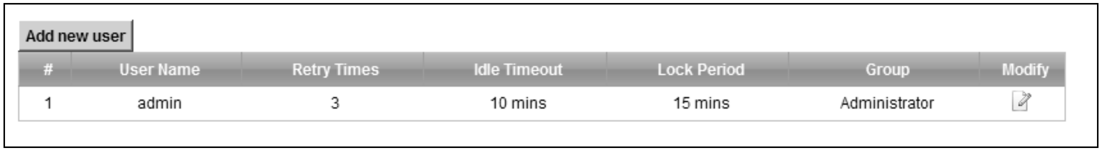
25.1 Overview

In the **Users Configuration** screen, you can view, add, and configure user accounts of the ZyXEL Device.

25.2 The Users Configuration Screen

Click **Maintenance > Users Configuration** to open the following screen.

Figure 113 Maintenance > Users Configuration



Add new user

#	User Name	Retry Times	Idle Timeout	Lock Period	Group	Modify
1	admin	3	10 mins	15 mins	Administrator	✎

The following table describes the labels in this screen.

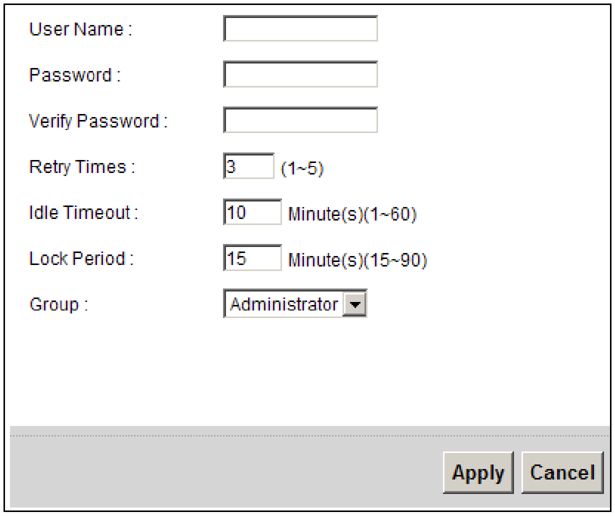
Table 92 Maintenance > Users Configuration

LABEL	DESCRIPTION
Add new user	Click this to configure a new user account.
#	This is the index number of the entry.
User Name	This field displays the name of the user.
Retry Times	This field indicates how many times a user can re-enter his/her account information before the ZyXEL Device locks the user out.
Idle Timeout	This field indicates the number of minutes that the system can idle before being logged out.
Lock Period	This field indicates the number of minutes for the lockout period. A user cannot log into the ZyXEL Device during the lockout period, even if he/she enters correct account information.
Group	This field displays the login account type of the user. Different login account types have different privilege levels. The web configurator screens and privileges vary depending on which account type you use to log in.
Modify	Click the **Edit** icon to edit this user account.

25.2.1 Add/Edit a Users Account

Use this screen to add or edit a users account. Click **Add new user** in the **Users Configuration** screen or the **Edit** icon next to the user account you want to edit. The screen shown next appears.

Figure 114 Users Configuration: Add/Edit



User Name :

Password :

Verify Password :

Retry Times : 3 (1~5)

Idle Timeout : 10 Minute(s)(1~60)

Lock Period : 15 Minute(s)(15~90)

Group : Administrator

The following table describes the labels in this screen.

Table 93 Users Configuration: Add/Edit

LABEL	DESCRIPTION
User Name	This field is read-only if you are editing the user account. Enter a descriptive name for the user account. The user name can be 6 to 15 alphanumeric characters (0-9, A-Z, a-z, -, _ with no spaces).
Password	Specify the password associated to this account. The password can be 6 to 15 alphanumeric characters (0-9, A-Z, a-z, -, _ with no spaces), not containing the user name. The characters are displayed as asterisks ¡§*¡¨ in this field.
Verify Password	Enter the exact same password that you just entered in the above field.
Retry Times	The ZyXEL Device can lock a user out if you use a wrong user name or password to log in the ZyXEL Device. Enter up to how many times a user can re-enter his/her account information before the ZyXEL Device locks the user out.
Idle Timeout	Enter the number of minutes that the system can idle before being logged out.
Lock Period	Enter the number of minutes for the lockout period. A user cannot log into the ZyXEL Device during the lockout period, even if he/she enters correct account information.

Table 93 Users Configuration: Add/Edit (continued)

LABEL	DESCRIPTION
Group	This field is read-only if you are editing the user account. Different login account types have different privilege levels. The web configurator screens and privileges vary depending on which account type you use to log in. Select a type of login account from the drop-down list box. The login account types include **Administrator** and **Security**. See Section 25.2.2 on page 259 for more information.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exit this screen without saving.

25.2.2 Types of Accounts

The ZyXEL Device provides two account types with different privilege levels. The web configurator screens vary depending on which account you use to log in. The following table describes the privileges of the different accounts.

Table 94 Types of Accounts

TYPE	PRIVILEGE
Administrator	• Create subscriber accounts. • View and configure associated devices. • Vendor configuration file management. • Device firmware upgrade. • Import device information to ZyXEL Device.
Security	• View information of devices assigned to the administrator who created this guest account.

26

Logs Setting

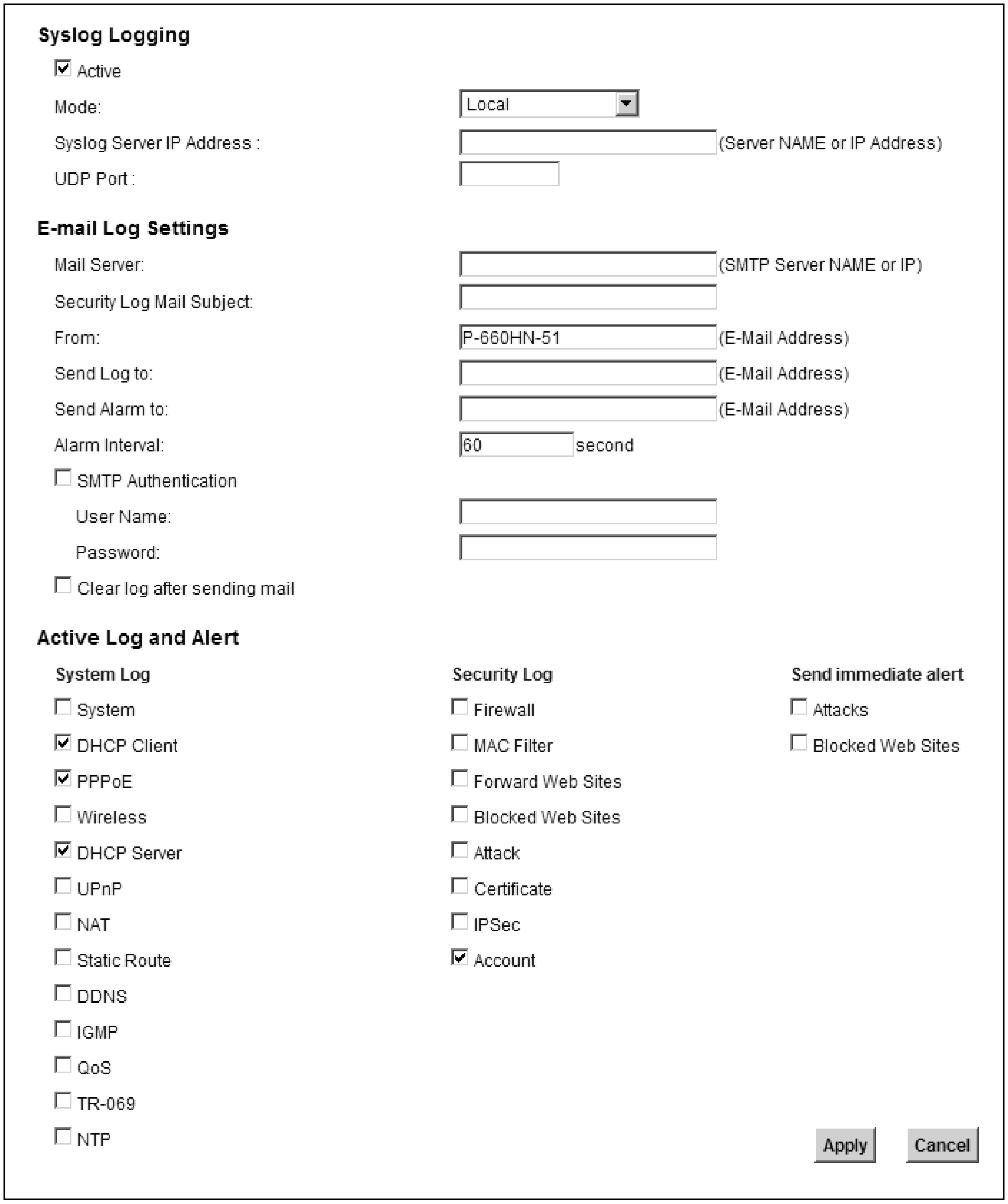
26.1 Overview

You can configure where the ZyXEL Device sends logs and which logs and/or immediate alerts the ZyXEL Device records in the **Logs Setting** screen.

26.2 The Log Settings Screen

To change your ZyXEL Device's log settings, click **Maintenance > Logs Setting**. The screen appears as shown.

Figure 115 Maintenance > Logs Setting



Syslog Logging

☑ Active

Mode:	Local ▾	
Syslog Server IP Address :		(Server NAME or IP Address)
UDP Port :		

E-mail Log Settings

Mail Server:		(SMTP Server NAME or IP)
Security Log Mail Subject:		
From:	P-660HN-51	(E-Mail Address)
Send Log to:		(E-Mail Address)
Send Alarm to:		(E-Mail Address)
Alarm Interval:	60	second
☐ SMTP Authentication		
User Name:		
Password:		
☐ Clear log after sending mail		

Active Log and Alert

System Log

☐ System
☑ DHCP Client
☑ PPPoE
☐ Wireless
☑ DHCP Server
☐ UPnP
☐ NAT
☐ Static Route
☐ DDNS
☐ IGMP
☐ QoS
☐ TR-069
☐ NTP

Security Log

☐ Firewall
☐ MAC Filter
☐ Forward Web Sites
☐ Blocked Web Sites
☐ Attack
☐ Certificate
☐ IPSec
☑ Account

Send immediate alert

☐ Attacks
☐ Blocked Web Sites

The following table describes the fields in this screen.

Table 95 Maintenance > Logs Setting

LABEL	DESCRIPTION
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Select the **Active** check box to enable syslog logging.

Table 95 Maintenance > Logs Setting (continued)

LABEL	DESCRIPTION
Mode	Select the syslog destination from the drop-down list box. If you select **Remote**, the log(s) will be sent to a remote syslog server. If you select **Local**, the log(s) will be saved in a local file. If you want to send the log(s) to a remote syslog server and save it in a local file, select **Remote and Local**.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
System Log Mail Subject	Type a title that you want to be in the subject line of the system log e-mail message that the ZyXEL Device sends.
Security Log Mail Subject	Type a title that you want to be in the subject line of the security log e-mail message that the ZyXEL Device sends.
From	Specify where the logs are sent from.
Send Log to	The ZyXEL Device sends logs to the e-mail address specified in this field. If this field is left blank, the ZyXEL Device does not send logs via E-mail.
Send Alarm to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
Alarm Interval	Specify how often the alarm should be updated.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one E-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the E-mail logs.
User Name	Enter the user name (up to 32 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Clear log after sending mail	Select this to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Active Log and Alert	
System Log	Select the categories of system logs that you want to record.
Security Log	Select the categories of security logs that you want to record.
Send immediate alert	Select log categories for which you want the ZyXEL Device to send E-mail alerts immediately.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

27

Firmware Upgrade

27.1 Overview

This chapter explains how to upload new firmware to your ZyXEL Device. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

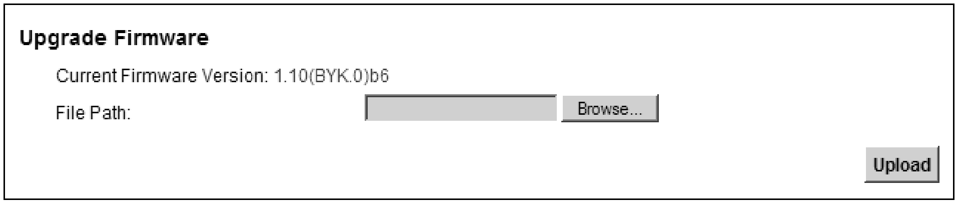
Only use firmware for your device's specific model. Refer to the label on the bottom of your ZyXEL Device.

27.2 The Firmware Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the ZyXEL Device while firmware upload is in progress!

Figure 116 Maintenance > Firmware Upgrade



Upgrade Firmware

Current Firmware Version: 1.10(BYK.0)b6

File Path:

The following table describes the labels in this screen.

Table 96 Maintenance > Firmware Upgrade

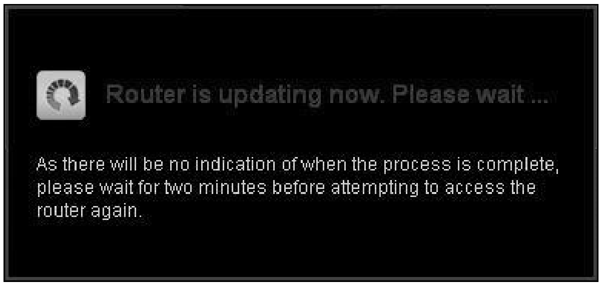
LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.

Table 96 Maintenance > Firmware Upgrade (continued)

LABEL	DESCRIPTION
Browse...	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

After you see the firmware updating screen, wait two minutes before logging into the ZyXEL Device again.

Figure 117 Firmware Uploading



Router is updating now. Please wait ...

As there will be no indication of when the process is complete, please wait for two minutes before attempting to access the router again.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

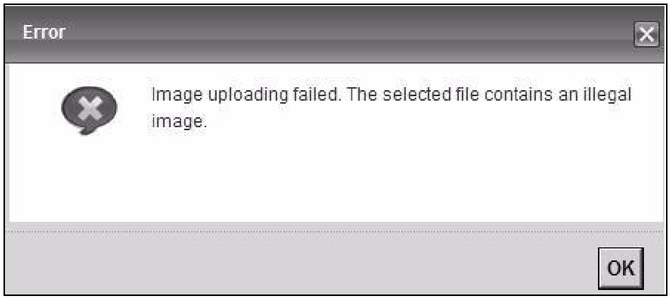
Figure 118 Network Temporarily Disconnected

Local Area Connection
Network cable unplugged

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 119 Error Message



Error

Image uploading failed. The selected file contains an illegal image.

28

Configuration

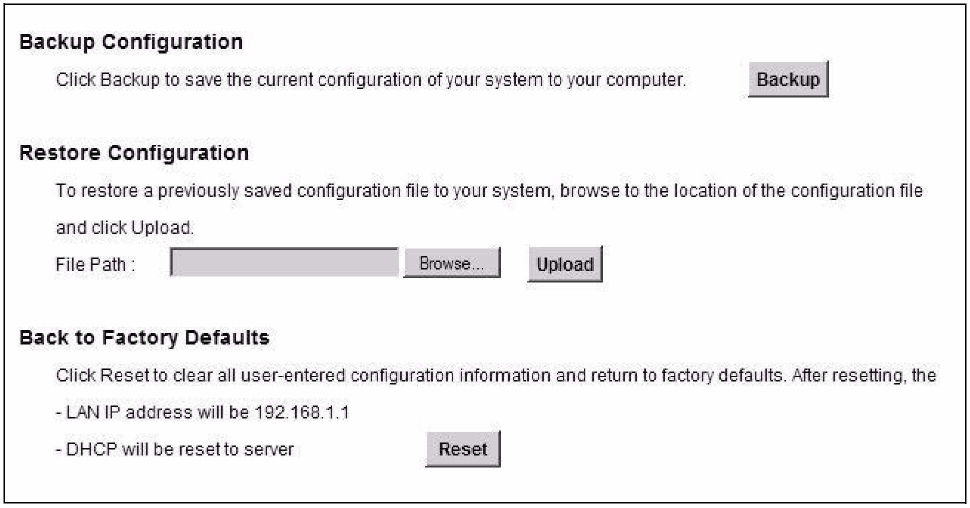
28.1 Overview

The **Configuration** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

28.2 The Configuration Screen

Click **Maintenance > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 120 Maintenance > Configuration



Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path :

Back to Factory Defaults

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the

- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

Backup Configuration

Backup Configuration allows you to back up (save) the ZyXEL Device’s current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyXEL Device's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

Table 97 Restore Configuration

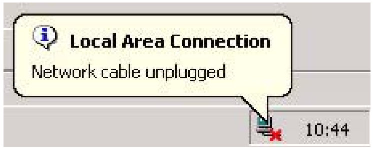
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.

Do not turn off the ZyXEL Device while configuration file upload is in progress.

After the ZyXEL Device configuration has been restored successfully, the login screen appears. Login again to restart the ZyXEL Device.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 121 Network Temporarily Disconnected



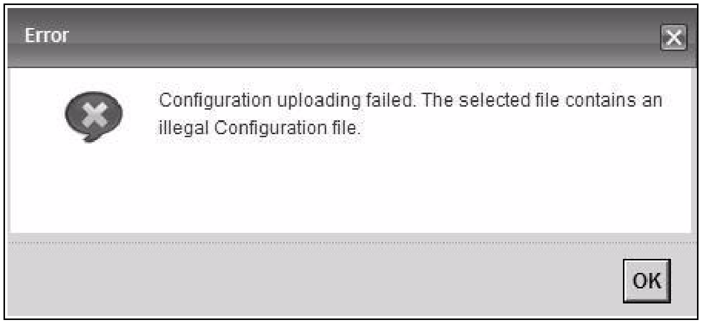
Local Area Connection

Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix A on page 287 for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **OK** to go back to the **Configuration** screen.

Figure 122 Configuration Upload Error

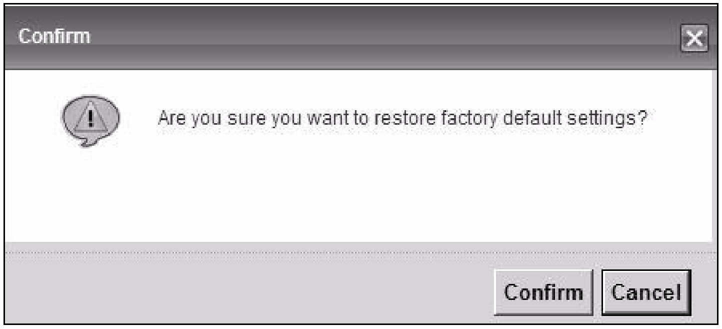


Configuration uploading failed. The selected file contains an illegal Configuration file.

Reset to Factory Defaults

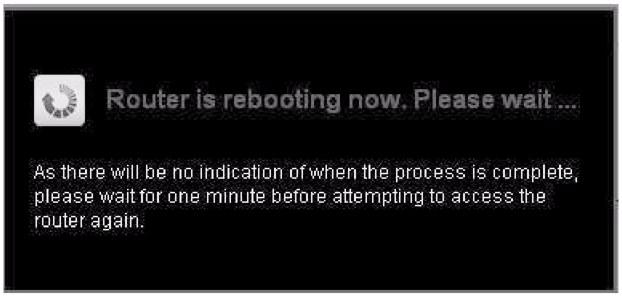
Click the **Reset** button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. The following warning screen appears.

Figure 123 Reset Warning Message



Are you sure you want to restore factory default settings?

Figure 124 Reset In Process Message



Router is rebooting now. Please wait ...

As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

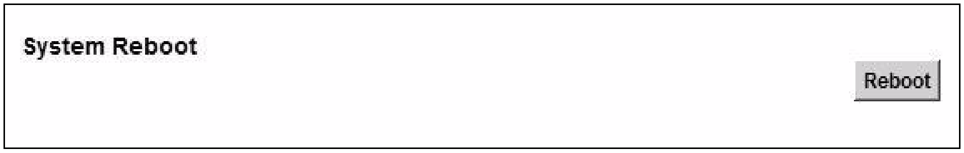
You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device. Refer to Section 1.7 on page 26 for more information on the **RESET** button.

28.3 The Reboot Screen

System restart allows you to reboot the ZyXEL Device remotely without turning the power off. You may need to do this if the ZyXEL Device hangs, for example.

Click **Maintenance > Reboot**. Click **Reboot** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

Figure 125 Maintenance > Reboot


System Reboot

29

Diagnostic

29.1 Overview

You can use different diagnostic methods to test a connection and see the detailed information. These read-only screens display information to help you identify problems with the ZyXEL Device.

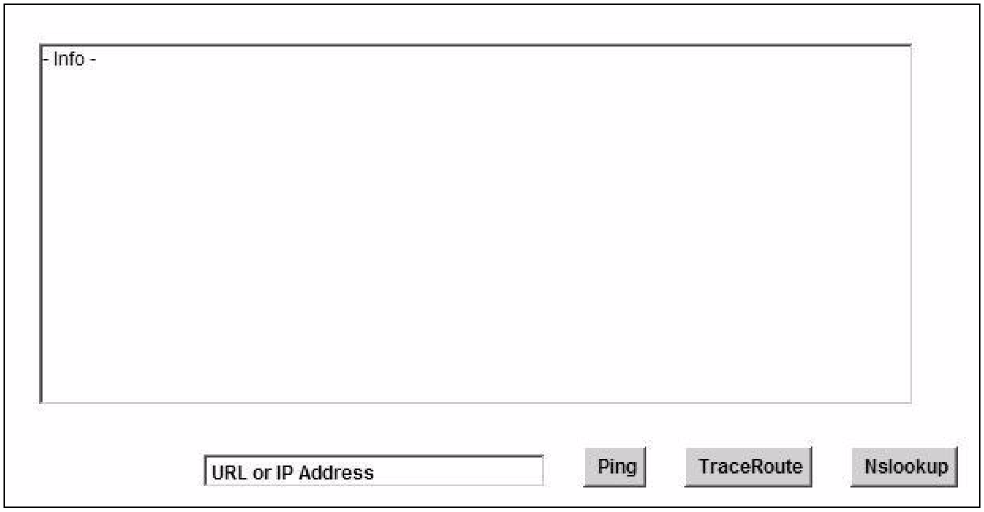
29.1.1 What You Can Do in this Chapter

- The **Ping & TraceRoute & NsLookup** screen lets you identify problems with the DSL connection. You can use Ping, TraceRoute, or Nslookup to help you identify problems.(Section 29.2 on page 271).
- The **OAM Ping Test** screen lets you send an ATM OAM (Operation, Administration and Maintenance) packet to verify the connectivity of a specific PVC. (Section 29.3 on page 272).

29.2 The Ping & TraceRoute & NsLookup Screen

Use this screen to ping, traceroute, or nslookup an IP address. Click **Maintenance > Diagnostic** to open the **Ping & TraceRoute & NsLookup** screen shown next.

Figure 126 Maintenance > Diagnostic > Ping & TraceRoute & NsLookup



The following table describes the fields in this screen.

Table 98 Maintenance > Diagnostic > Ping & TraceRoute & NsLookup

LABEL	DESCRIPTION
URL or IP Address	Type the IP address of a computer that you want to perform ping, traceroute, or nslookup in order to test a connection.
Ping	Click this to ping the IP address that you entered.
TraceRoute	Click this button to perform the traceroute function. This determines the path a packet takes to the specified computer.
Nslookup	Click this button to perform a DNS lookup on the IP address of a computer you enter.

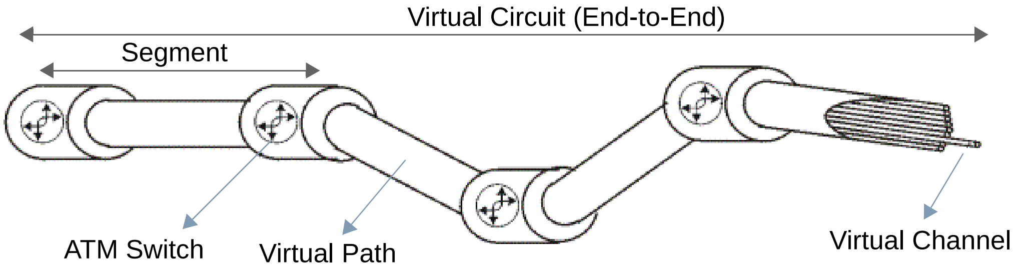
29.3 The OAM Ping Test Screen

Click **Maintenance > Diagnostic > OAM Ping Test** to open the screen shown next. Use this screen to perform an OAM (Operation, Administration and Maintenance) F4 or F5 loopback test on a PVC. The ZyXEL Device sends an OAM F4 or F5 packet to the DSLAM or ATM switch and then returns it to the ZyXEL Device. The test result then displays in the text box.

ATM sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

• Virtual Channel (VC)	Logical connections between ATM devices
• Virtual Path (VP)	A bundle of virtual channels
• Virtual Circuits	A series of virtual paths between circuit end points

Figure 127 Virtual Circuit Topology



Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path. A series of virtual paths make up a virtual circuit.

F4 cells operate at the virtual path (VP) level, while F5 cells operate at the virtual channel (VC) level. F4 cells use the same VPI as the user data cells on VP connections, but use different predefined VCI values. F5 cells use the same VPI and VCI as the user data cells on the VC connections, and are distinguished from data cells by a predefinded Payload Type Identifier (PTI) in the cell header. Both F4 flows and F5 flows are bidirectional and have two types.

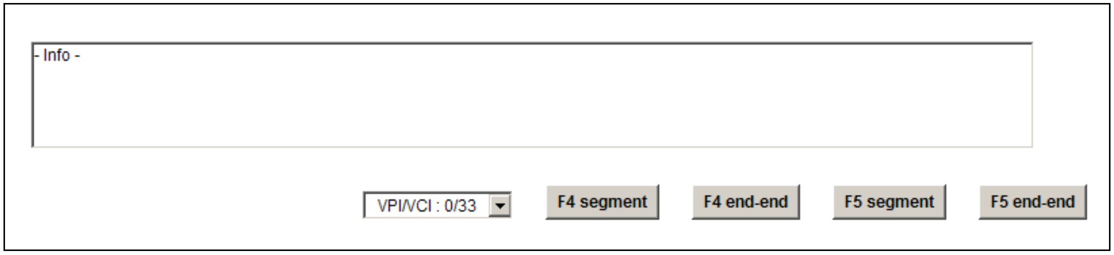
- segment F4 flows (VCI=3)
- end-to-end F4 flows (VCI=4)
- segment F5 flows (PTI=100)
- end-to-end F5 flows (PTI=101)

OAM F4 or F5 tests are used to check virtual path or virtual channel availbility between two DSL devices. Segment flows are terminated at the connecting point which terminates a VP or VC segment. End-to-end flows are terminated at the end point of a VP or VC connection, where an ATM link is terminated. Segment loopback tests allow you to verify integrity of a PVC to the nearest neighboring ATM device. End-to-end loopback tests allow you to verify integrity of an end-to-end PVC.

Note: The DSLAM to which the ZyXEL Device is connected must also support ATM F4 and/or F5 to use this test.

Note: This screen is available only when you configure an ATM layer-2 interface.

Figure 128 Maintenance > Diagnostic > OAM Ping Test



The following table describes the fields in this screen.

Table 99 Maintenance > Diagnostic > OAM Ping Test

LABEL	DESCRIPTION
	Select a PVC on which you want to perform the loopback test.
F4 segment	Press this to perform an OAM F4 segment loopback test.
F4 end-end	Press this to perform an OAM F4 end-to-end loopback test.
F5 segment	Press this to perform an OAM F5 segment loopback test.
F5 end-end	Press this to perform an OAM F5 end-to-end loopback test.

30

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access

30.1 Power, Hardware Connections, and LEDs

The ZyXEL Device does not turn on. None of the LEDs turn on.

1. Make sure the ZyXEL Device is turned on.
2. Make sure you are using the power adaptor or cord included with the ZyXEL Device.
3. Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the ZyXEL Device off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.6 on page 25.

2 Check the hardware connections.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the ZyXEL Device off and on.

5 If the problem continues, contact the vendor.

30.2 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

1 The default IP address is **192.168.1.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.7 on page 26.

I forgot the password.

1 The default admin password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 1.7 on page 26.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.

- If you changed the IP address (Section 7.2 on page 116), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix B on page 311.

4 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See Section 1.7 on page 26.

5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings and firewall rules to find out why the ZyXEL Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

1 Make sure you have entered the password correctly. The default admin password is **1234**. The field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.

3 Turn the ZyXEL Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 30.1 on page 275.

I cannot Telnet to the ZyXEL Device.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

30.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.6 on page 25.
2. Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
4. If you are trying to access the Internet wirelessly, make sure you have enabled the wireless LAN by the **WPS** button or the **Network Settings > Wireless > General** screen.
5. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
6. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.6 on page 25.
2. Turn the ZyXEL Device off and on.
3. If the problem continues, contact your ISP.

30.4 Wireless Internet Access

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

What is a Server Set ID (SSID)?

An SSID is a name that uniquely identifies a wireless network. The AP and all the clients within a wireless network must use the same SSID.

What wireless security modes does my ZyXEL Device support?

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

The available security modes in your ZyXEL device are as follows:

- **WPA2-PSK:** (recommended) This uses a pre-shared key with the WPA2 standard.
- **WPA-PSK:** This has the device use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
- **WPA2:** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. It requires the use of a RADIUS server and is mostly used in business networks.
- **WPA:** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. It requires the use of a RADIUS server and is mostly used in business networks.
- **WEP:** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.

31

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

31.1 Hardware Specifications

Table 100 Hardware Specifications

Dimensions	188(H) x 40(W) x 132(D) mm
Weight	374 g
Power Specification	12VDC 1A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
ADSL Port	1 RJ-11 FXS POTS port
RESET Button	Restores factory defaults
Antenna	2 internal antennas, 2dBi
WPS Button	1 second: turn on or off WLAN 5 seconds: enable WPS (Wi-Fi Protected Setup)
Operation Temperature	0º C ~ 40º C
Storage Temperature	-25º ~ 65º C
Operation Humidity	20% ~ 90% RH
Storage Humidity	20% ~ 90% RH

31.2 Firmware Specifications

Table 101 Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)

Table 101 Firmware Specifications (continued)

Default Admin Password	1234
DHCP Server IP Pool	192.168.1.64 to 192.168.1.253
Device Management	Use the web configurator to easily configure the rich range of features on the ZyXEL Device.
Wireless Functionality	Allow the IEEE 802.11b/g/n wireless clients to connect to the ZyXEL Device wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting. You can send logs from the ZyXEL Device to an external syslog server.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
Firewall	Your device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
Content Filtering	URL filtering allows you to block access to Internet web sites of certain URL that you specify.

Table 101 Firmware Specifications (continued)

QoS (Quality of Service)	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyXEL Device.
PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Other PPPoE Features	PPPoE idle time out PPPoE dial on demand
Multiple PVC (Permanent Virtual Circuits) Support	Your device supports up to 8 Permanent Virtual Circuits (PVCs).
Packet Filters	Your device's packet filtering function allows added network security and management.
ADSL Standards	Support Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1) FDM-mode per ANSI T1.413 and ITU-T G.992.1 ADSL2 G.dmt.bis (G.992.3) ADSL2+ (G.992.5) Reach Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Support multi-protocol over AAL5 (RFC2684/1483) Support PPP over ATM AAL5 (RFC2364) PPP over Ethernet support for DSL connection (RFC 2516) Support VC-based and LLC-based multiplexing Support up to 8 PVCs I.610 F4/F5 OAM TR-067/TR-100 supported

Table 101 Firmware Specifications (continued)

Other Protocol Support	Dynamic DNS (www.dyndns.org) DHCP client/server/relay IGMP v1, v2, and v3 IP Policy Routing UPnP support Transparent bridging, VLAN-tagging pass-through bridge mode Static DHCP
Management	Embedded Web Configurator TR-069 HTTPS

31.3 Wireless Features

Table 102 Wireless Features

Internal Antennas	The ZyXEL Device is equipped with two internal antennas to provide a clear radio signal between the wireless stations and the access points.
Wireless LAN MAC Address Filtering	Your device can check the MAC addresses of wireless stations against a list of allowed or denied MAC addresses.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.
Wi-Fi Protected Access	Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security standard. Key differences between WPA and WEP are user authentication and improved data encryption.
WPA2	WPA 2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Table 102 Wireless Features

WMM QoS	WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic according to the delivery requirements of individual services.
Other Wireless Features	WDS support IEEE 802.11n Compliance Frequency Range:2.4 GHz Advanced Orthogonal Frequency Division Multiplexing (OFDM) Max physical rate: 150Mbps for 1x1 11n Max physical rate: 300Mbps for 2x2 11n EIRP: 26dBm WEP, TKIP, AES Data Encryption WLAN bridge to LAN 32 MAC Address filter WPA, WPA-PSK, WPA2, WPA2-PSK WPS IEEE 802.1x (EAP-TLS) WMM WDS Multi BSSID (4 BSSIDs) Wireless Scheduling Auto-channel selection Output power adjustment

The following list, which is not exhaustive, illustrates the standards supported in the ZyXEL Device.

Table 103 Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)

Table 103 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2364	PPP over AAL5 (PPP over ATM over ADSL)
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5.
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/ WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11n	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard.
G dmt(G.992.1)	G.992.1 Asymmetrical Digital Subscriber Line (ADSL) Transceivers
ITU G.992.1 (G.DMT)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.2 (G. Lite)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.3 (G.dmt.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.5 (ADSL2+)	ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits.
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)
MBM v2	Media Bandwidth Management v2
RFC 2383	ST2+ over ATM Protocol Specification - UNI 3.1 Version
TR-069	TR-069 DSL Forum Standard for CPE Wan Management.
1.363.5	Compliant AAL5 SAR (Segmentation And Re-assembly)

A

Setting up Your Computer’s IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

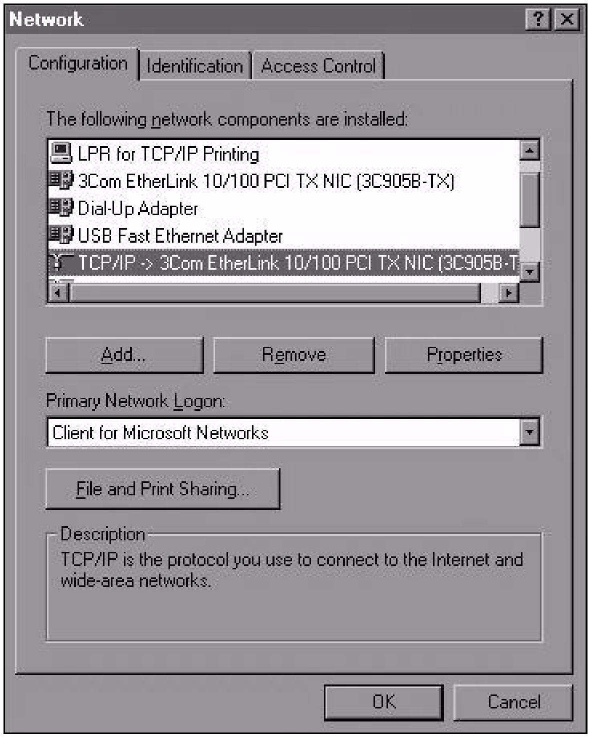
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyXEL Device’s LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 129 WIndows 95/98/Me: Network: Configuration



The following network components are installed:

- LPR for TCP/IP Printing
- 3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
- Dial-Up Adapter
- USB Fast Ethernet Adapter
- TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon: Client for Microsoft Networks

Description

TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.

2 Select **Adapter** and then click **Add**.

3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.

2 Select **Protocol** and then click **Add**.

3 Select **Microsoft** from the list of **manufacturers**.

4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.

2 Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

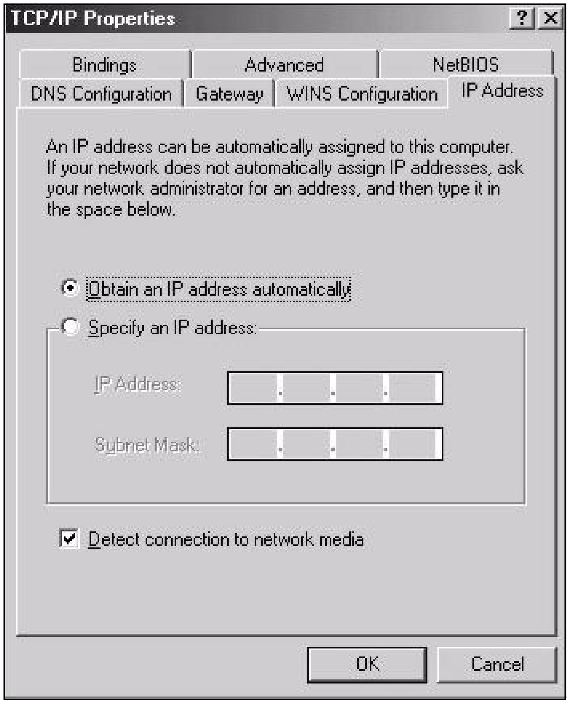
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 130 Windows 95/98/Me: TCP/IP Properties: IP Address



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

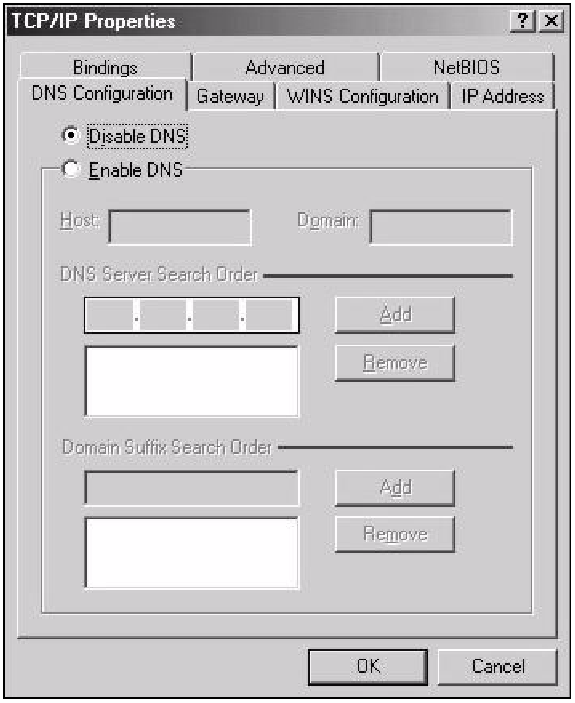
Subnet Mask: . . .

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 131 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your ZyXEL Device and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

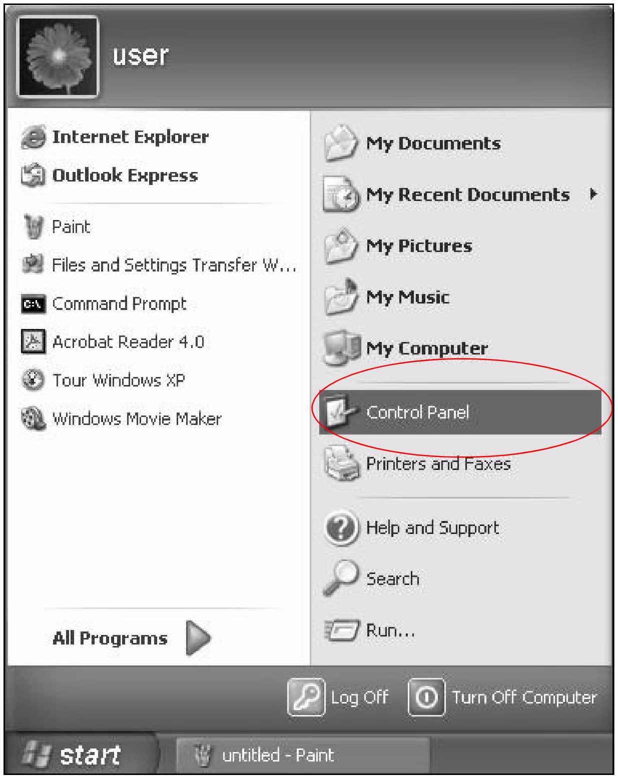
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

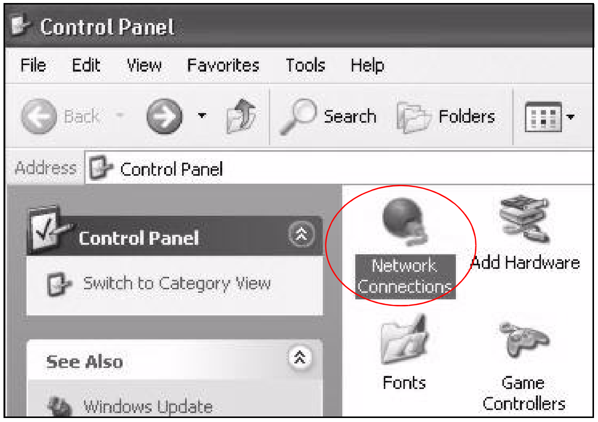
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 132 Windows XP: Start Menu



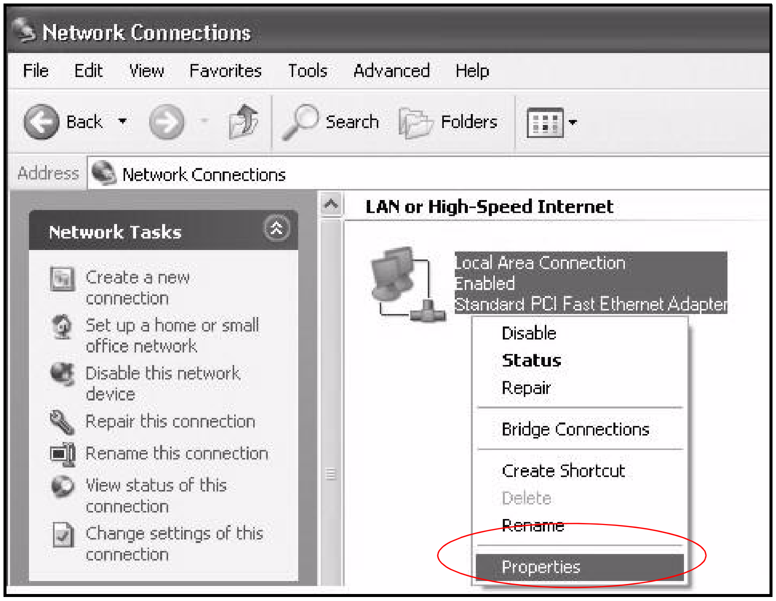
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 133 Windows XP: Control Panel



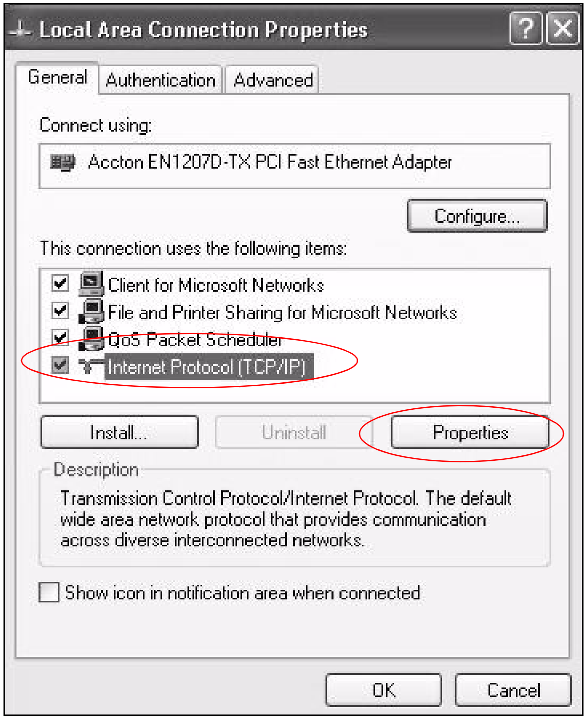
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 134 Windows XP: Control Panel: Network Connections: Properties


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
LAN or High-Speed Internet
Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter
Disable
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties

4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 135 Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

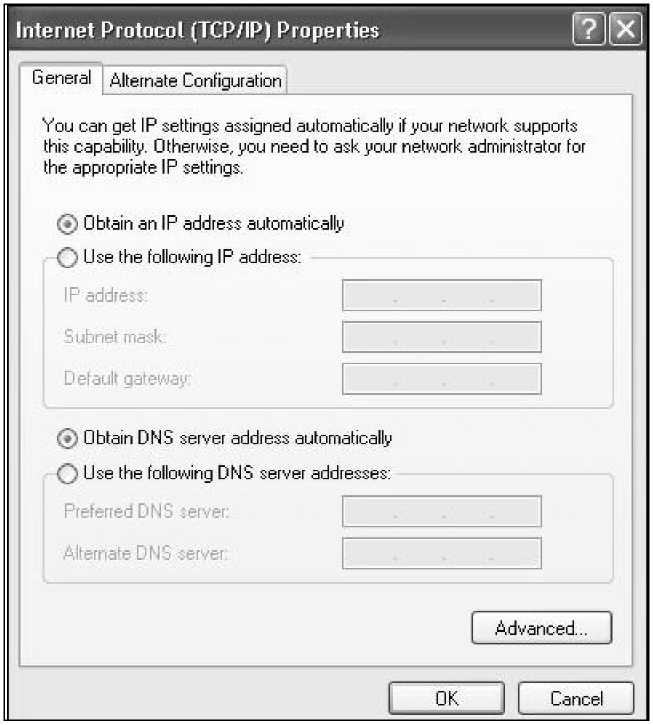
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 136 Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

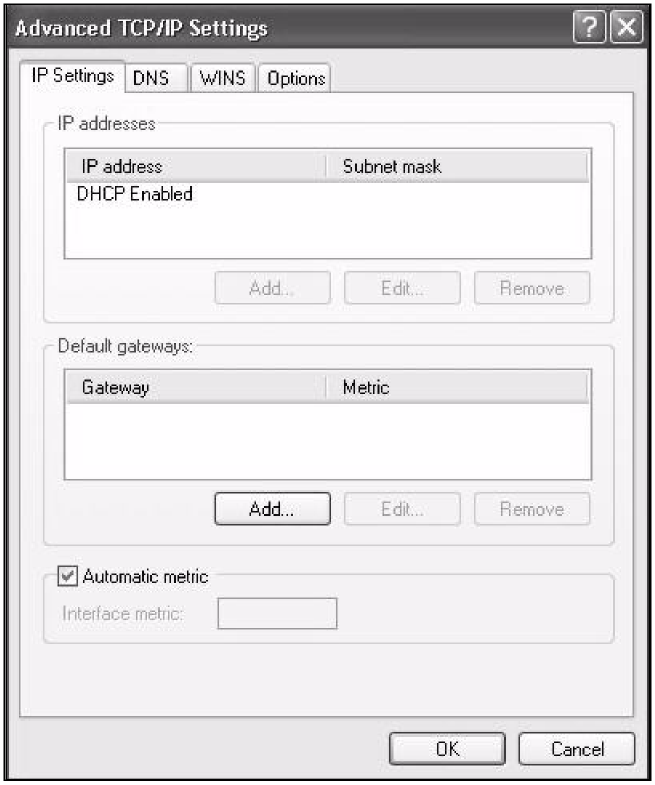
6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

Figure 137 Windows XP: Advanced TCP/IP Properties



DHCP Enabled

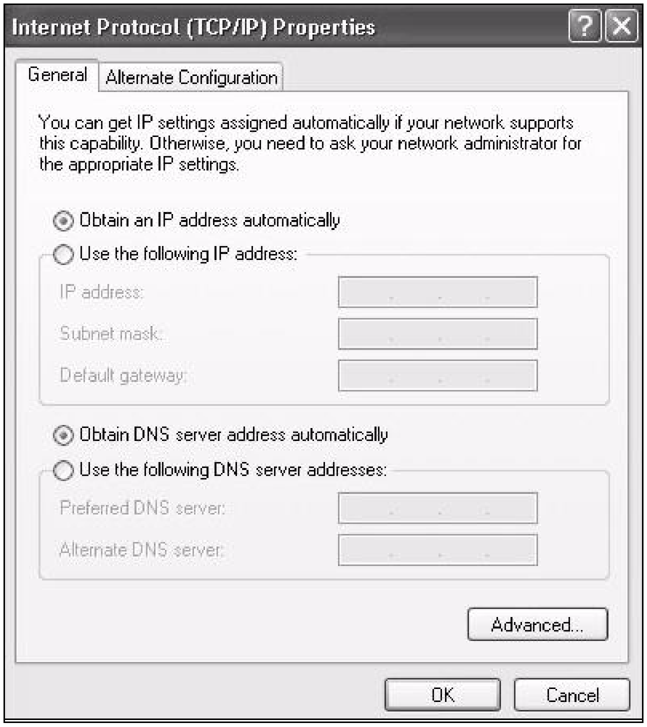
☑ Automatic metric

7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 138 Windows XP: Internal Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

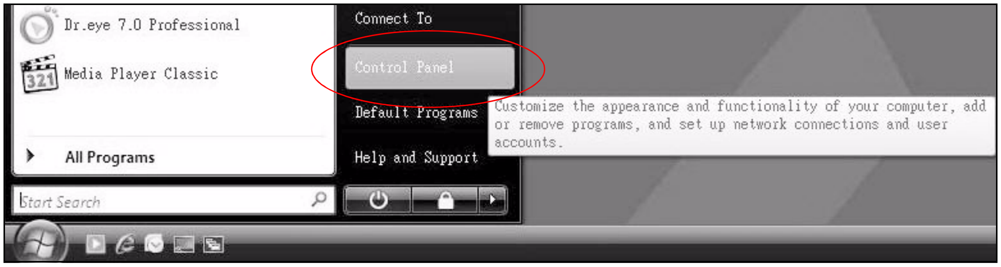
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Windows Vista

This section shows screens from Windows Vista Enterprise Version 6.0.

1 Click the **Start** icon, **Control Panel**.

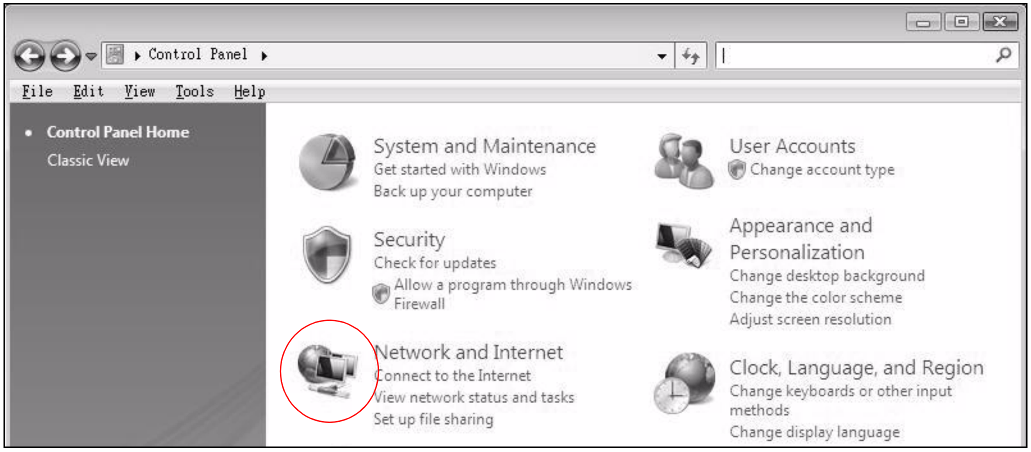
Figure 139 Windows Vista: Start Menu



Customize the appearance and functionality of your computer, add or remove programs, and set up network connections and user accounts.

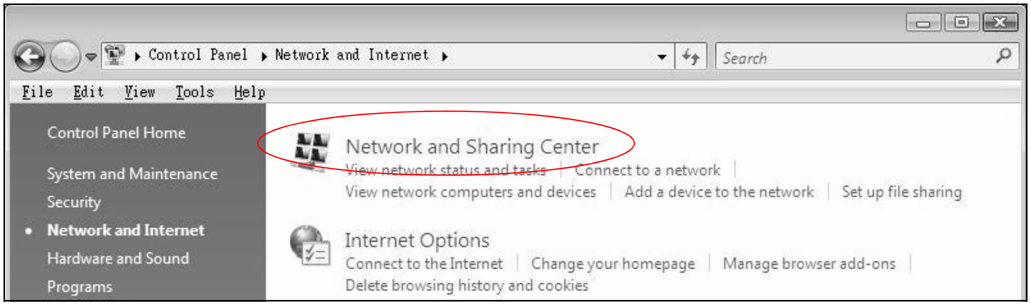
2 In the **Control Panel**, double-click **Network and Internet**.

Figure 140 Windows Vista: Control Panel



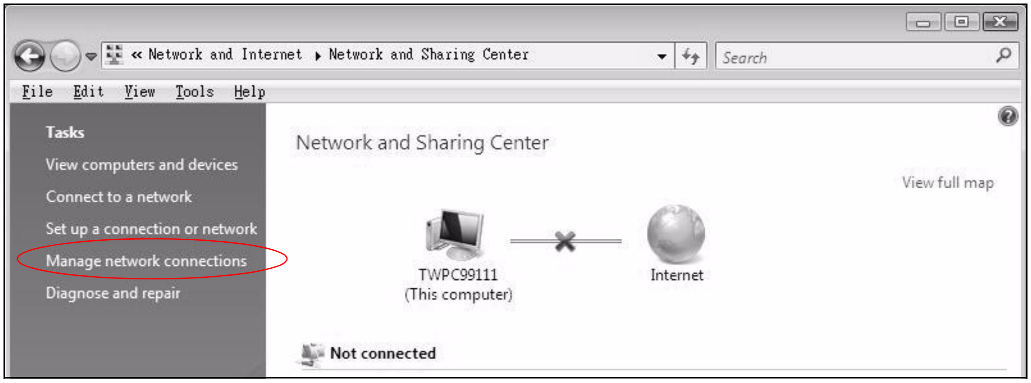
3 Click **Network and Sharing Center**.

Figure 141 Windows Vista: Network And Internet



4 Click **Manage network connections**.

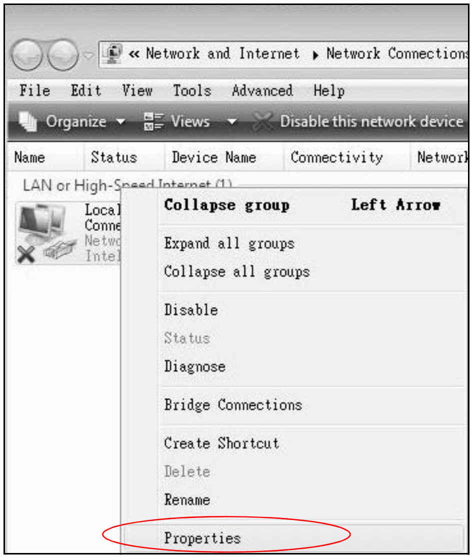
Figure 142 Windows Vista: Network and Sharing Center


« Network and Internet ▸ Network and Sharing Center
Search
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
Network and Sharing Center
View full map
TWPC99111
(This computer)
Internet
Not connected

5 Right-click **Local Area Connection** and then click **Properties**.

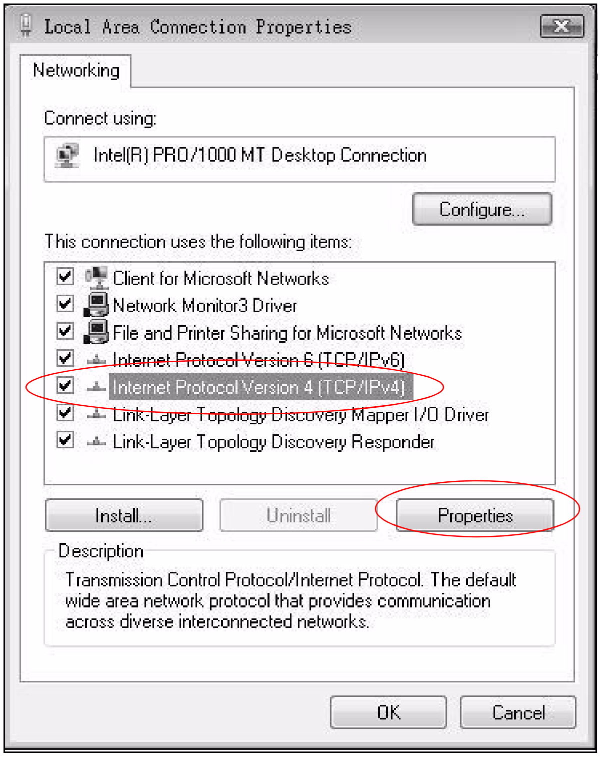
Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

Figure 143 Windows Vista: Network and Sharing Center


« Network and Internet ▸ Network Connections
File Edit View Tools Advanced Help
Organize Views Disable this network device
Name Status Device Name Connectivity Network
LAN or High-Speed Internet (1)
Local
Conne
Netwo
Intel
Collapse group Left Arrow
Expand all groups
Collapse all groups
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties

6 Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

Figure 144 Windows Vista: Local Area Connection Properties



Connect using:

Intel(R) PRO/1000 MT Desktop Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Network Monitor3 Driver
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

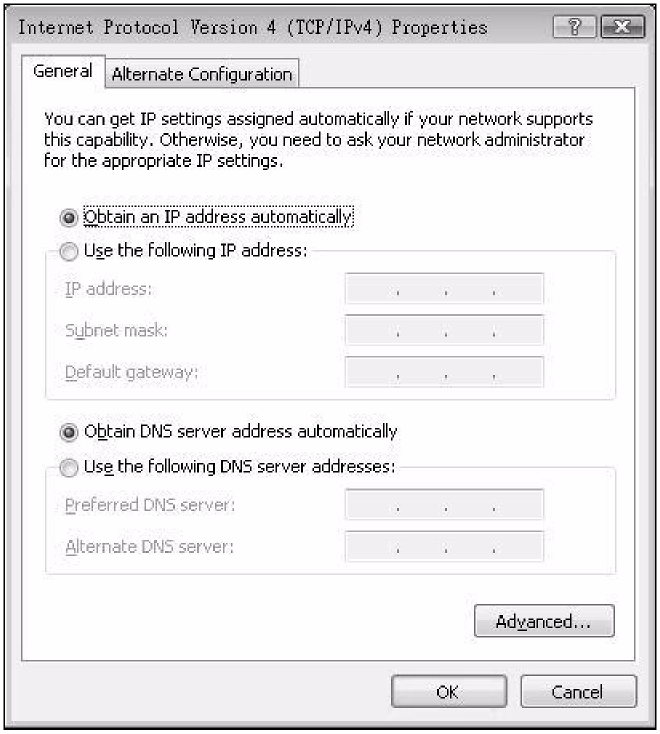
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens (the **General tab**).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

- Click **Advanced**.

Figure 145 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

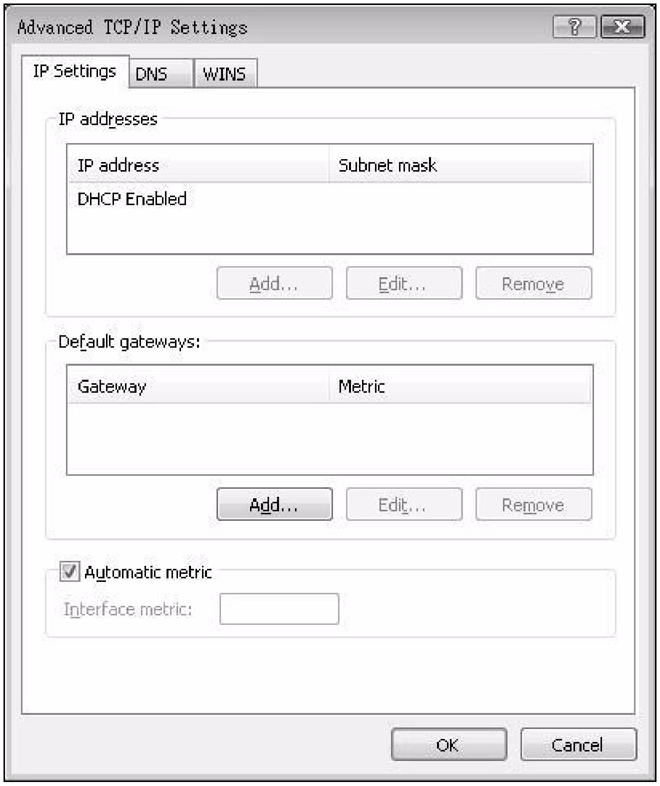
8 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

Figure 146 Windows Vista: Advanced TCP/IP Properties

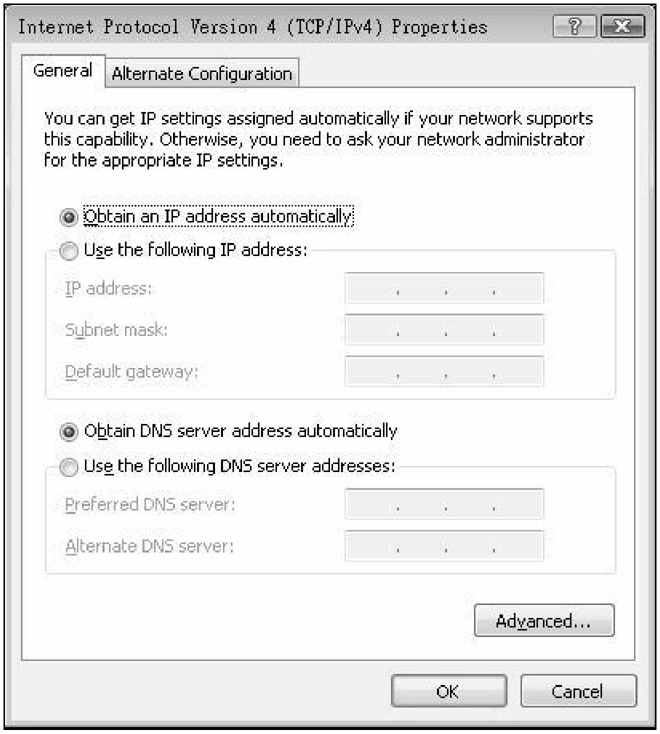


9 In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, (the **General tab**):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 147 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

10 Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

11 Click **Close** to close the **Local Area Connection Properties** window.

12 Close the **Network Connections** window.

13 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

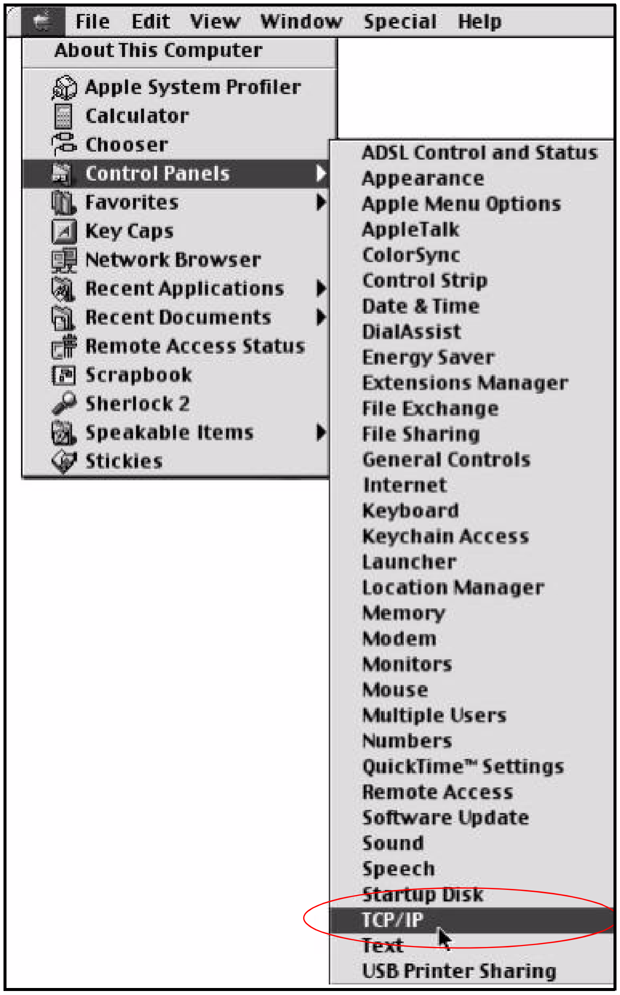
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

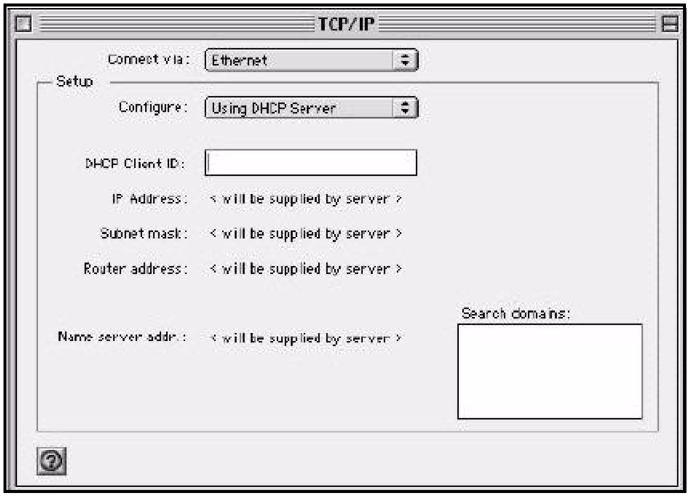
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 148 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 149 Macintosh OS 8/9: TCP/IP



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Search domains:

Name server addr.: < will be supplied by server >

3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your ZyXEL Device and restart your computer (if prompted).

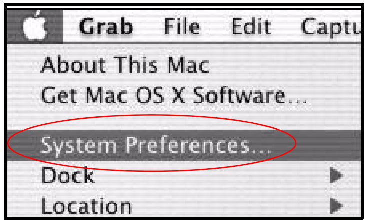
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 150 Macintosh OS X: Apple Menu

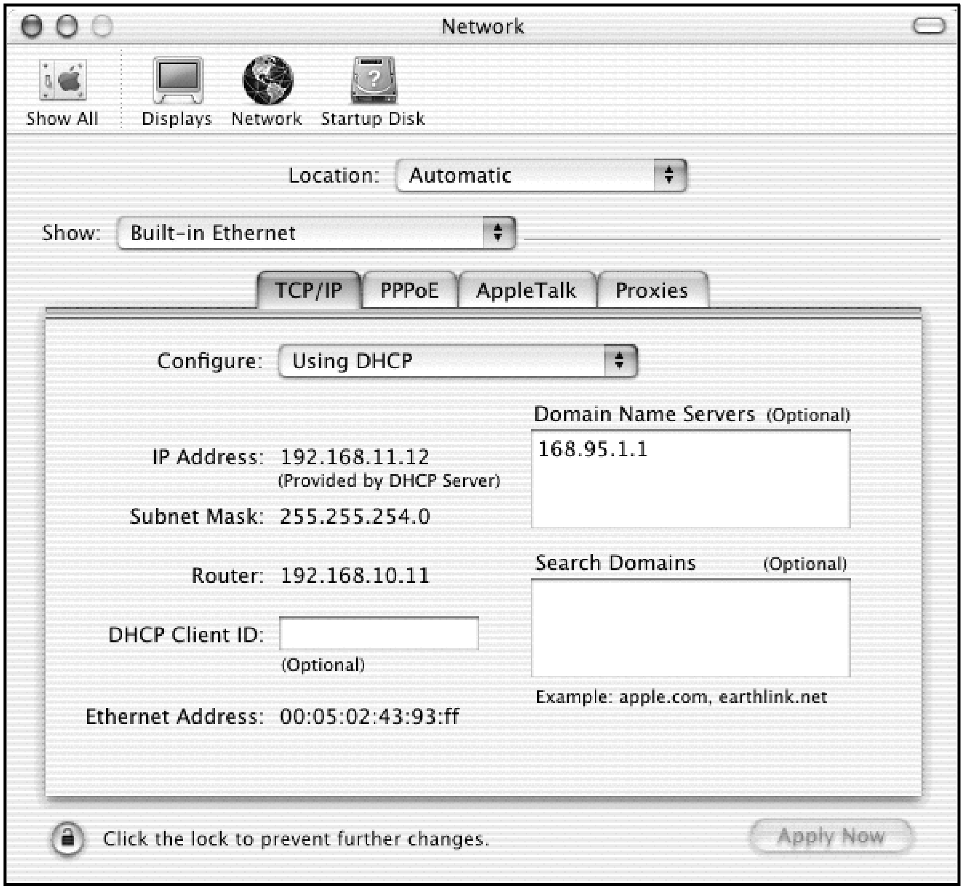


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 151 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer’s TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

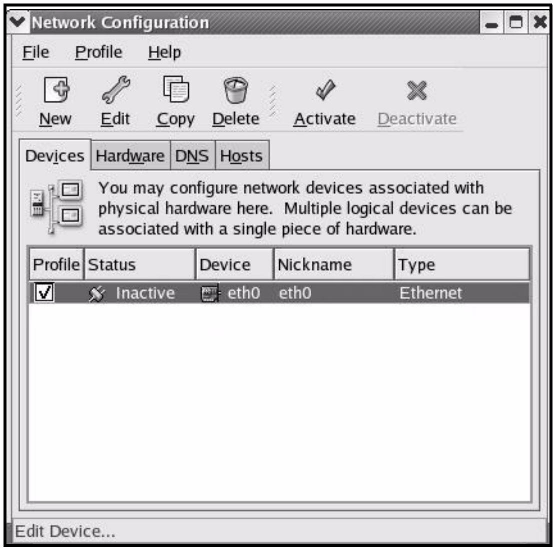
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 152 Red Hat 9.0: KDE: Network Configuration: Devices

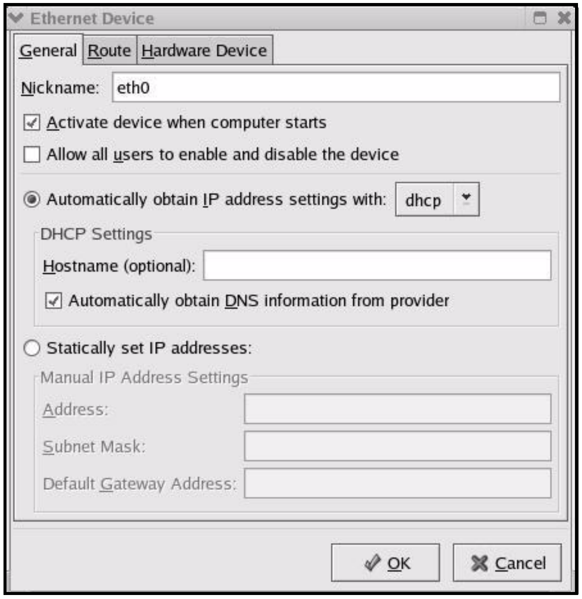


You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

Profile	Status	Device	Nickname	Type
☑	Inactive	eth0	eth0	Ethernet

2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 153 Red Hat 9.0: KDE: Ethernet Device: General



Nickname: eth0

☑ Activate device when computer starts

□ Allow all users to enable and disable the device

● Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

☑ Automatically obtain DNS information from provider

○ Statically set IP addresses:

Manual IP Address Settings

Address:

Subnet Mask:

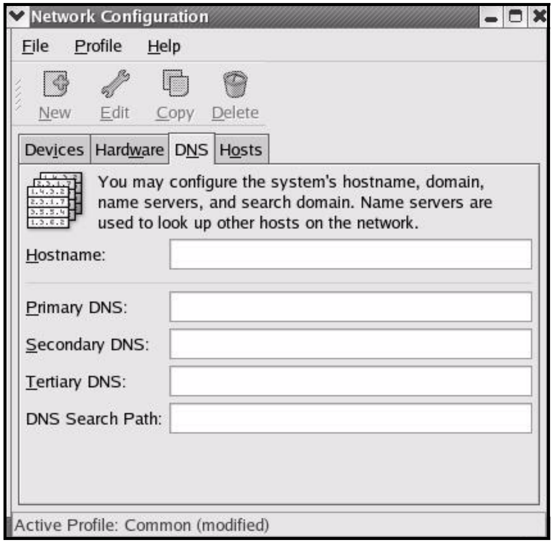
Default Gateway Address:

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 154 Red Hat 9.0: KDE: Network Configuration: DNS



You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

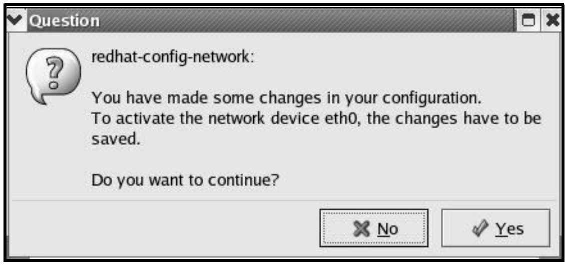
DNS Search Path:

Active Profile: Common (modified)

5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 155 Red Hat 9.0: KDE: Network Configuration: Activate



redhat-config-network:

You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.

Do you want to continue?

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 156 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the BOOTPROTO= field. Type IPADDR= followed by the IP address (in dotted decimal notation) and type NETMASK= followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 157 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the resolv.conf file in the /etc directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 158 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter ./network restart in the /etc/rc.d/init.d directory. The following figure shows an example.

Figure 159 Red Hat 9.0: Restart Ethernet Card

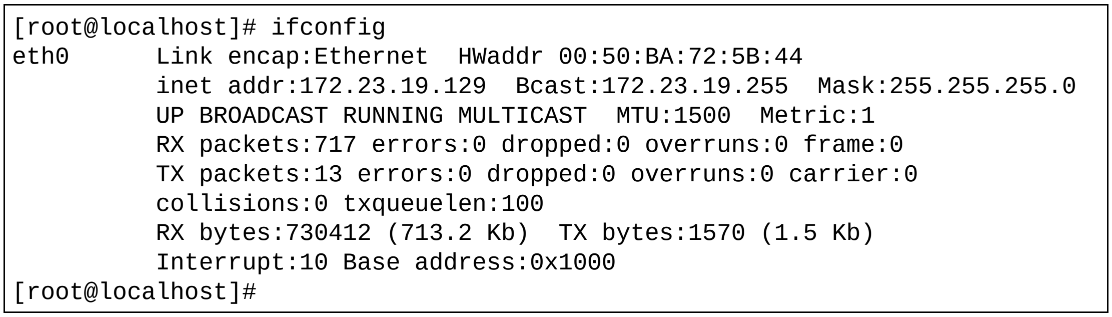
```
[root@localhost init.d]# network restart

Shutting down interface eth0:                  [OK]
Shutting down loopback interface:              [OK]
Setting network parameters:                    [OK]
Bringing up loopback interface:                [OK]
Bringing up interface eth0:                    [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 160 Red Hat 9.0: Checking TCP/IP Properties



```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

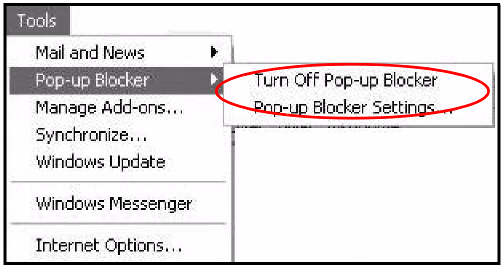
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 161 Pop-up Blocker

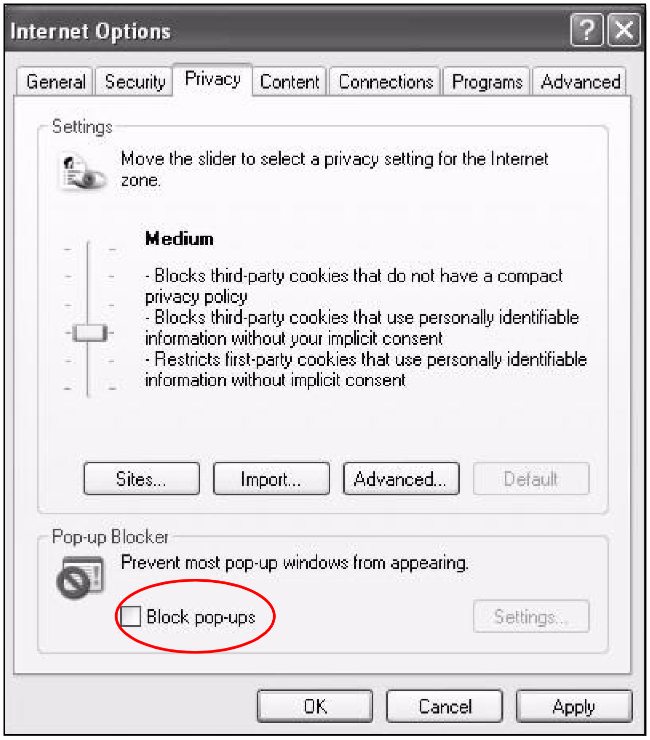


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 162 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

□ Block pop-ups

3 Click **Apply** to save this setting.

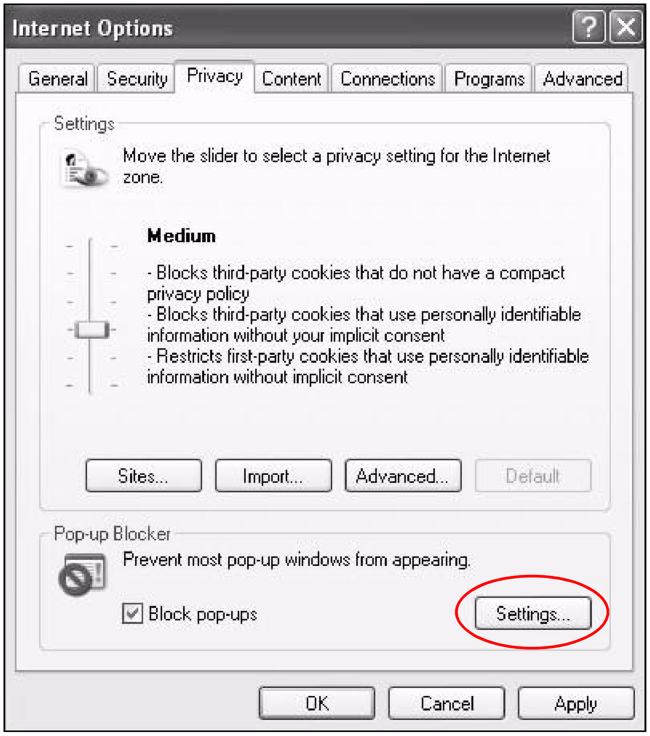
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 163 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

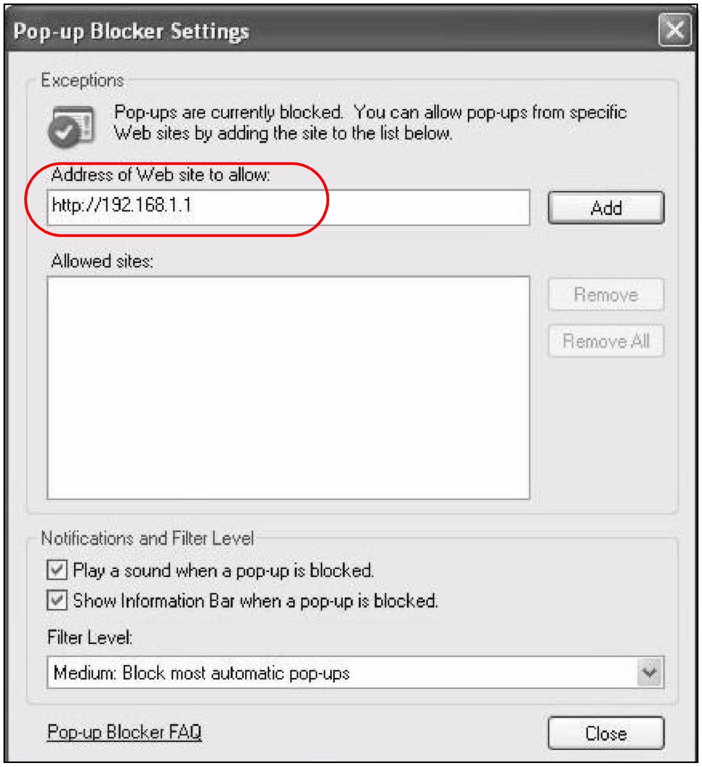
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 164 Pop-up Blocker Settings



Pop-up Blocker Settings

Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow: http://192.168.1.1

Allowed sites:

Notifications and Filter Level

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

5 Click **Close** to return to the **Privacy** screen.

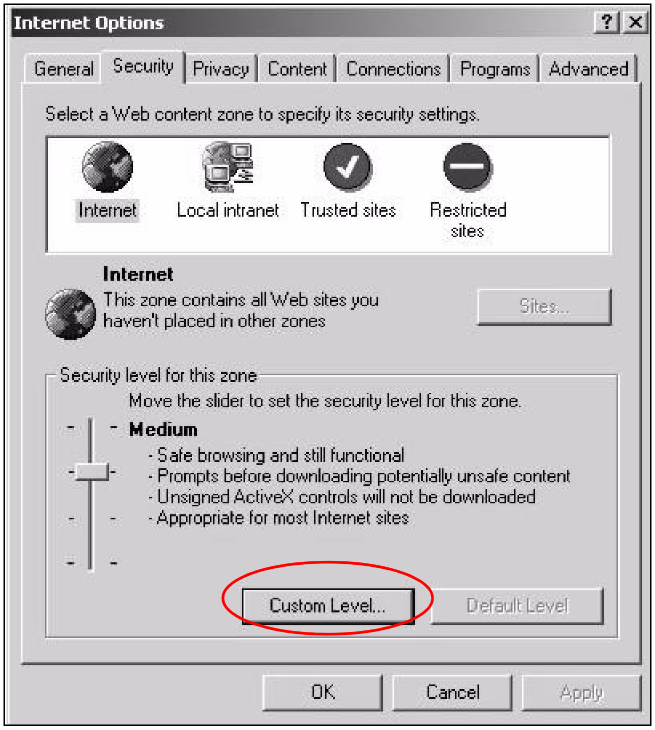
6 Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 165 Internet Options: Security



Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Select a Web content zone to specify its security settings.
Internet
Local intranet
Trusted sites
Restricted sites
Internet
This zone contains all Web sites you haven't placed in other zones
Sites...
Security level for this zone
Move the slider to set the security level for this zone.
Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites
Custom Level...
Default Level
OK
Cancel
Apply

2 Click the **Custom Level...** button.

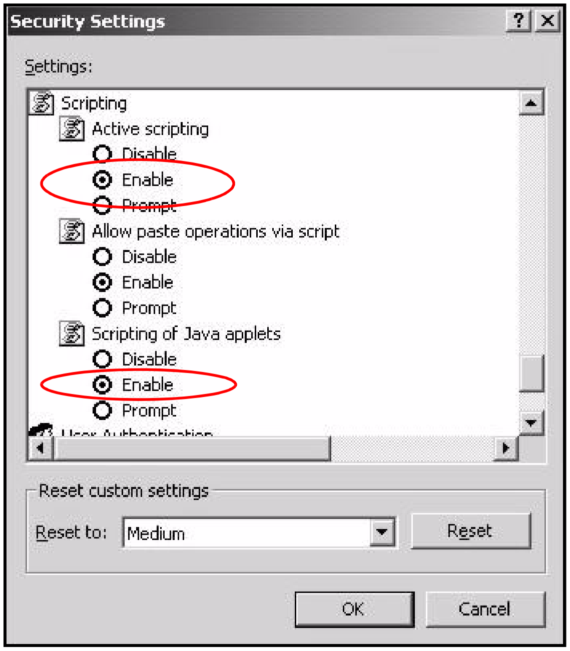
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 166 Security Settings - Java Scripting



Security Settings

Settings:

- Scripting
  - Active scripting
    - ○ Disable
    - ● Enable
    - ○ Prompt
  - Allow paste operations via script
    - ○ Disable
    - ● Enable
    - ○ Prompt
  - Scripting of Java applets
    - ○ Disable
    - ● Enable
    - ○ Prompt
- User Authentication

Reset custom settings

Reset to: Medium

Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

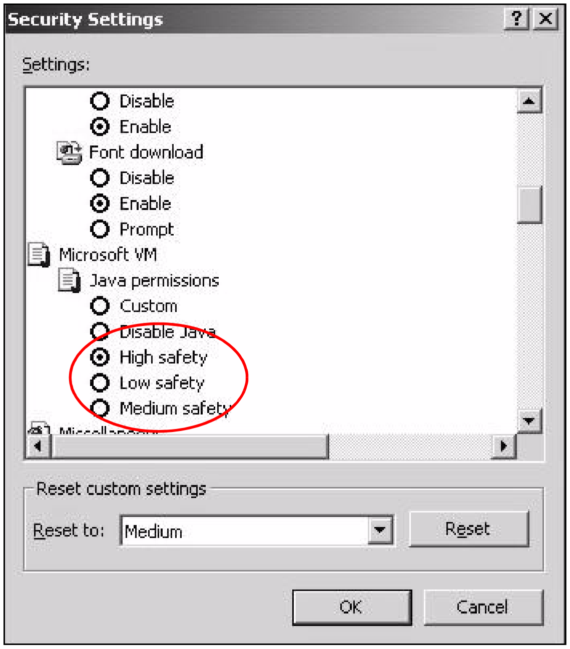
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 167 Security Settings - Java



Security Settings

Settings:

- ○ Disable
- ● Enable
- Font download
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Microsoft VM
  - Java permissions
    - ○ Custom
    - ○ Disable Java
    - ● High safety
    - ○ Low safety
    - ○ Medium safety

Reset custom settings

Reset to: Medium

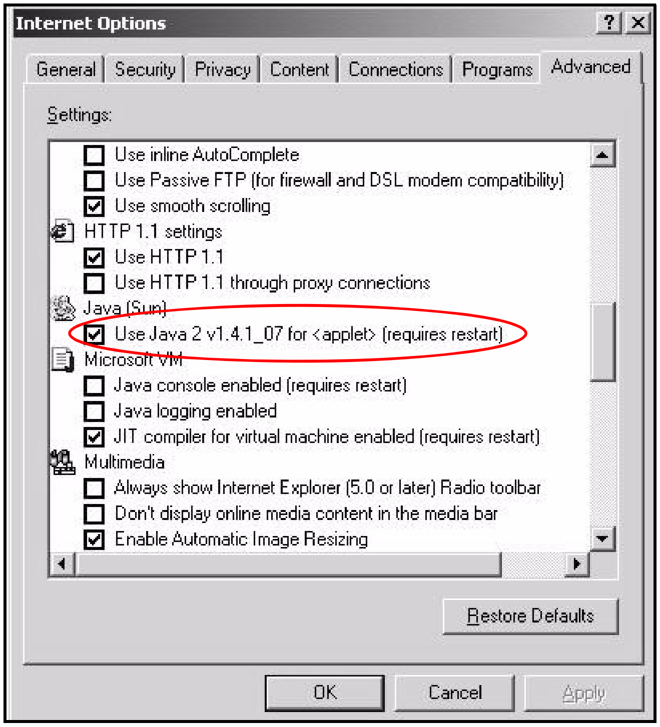
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 168 Java (Sun)



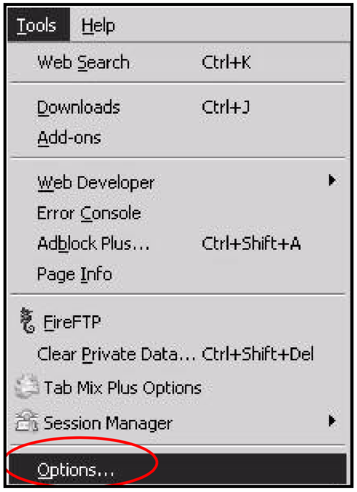
☐ Use inline AutoComplete
☐ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
☐ Use HTTP 1.1 through proxy connections
Java (Sun)
☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
Microsoft VM
☐ Java console enabled (requires restart)
☐ Java logging enabled
☑ JIT compiler for virtual machine enabled (requires restart)
Multimedia
☐ Always show Internet Explorer (5.0 or later) Radio toolbar
☐ Don't display online media content in the media bar
☑ Enable Automatic Image Resizing

Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

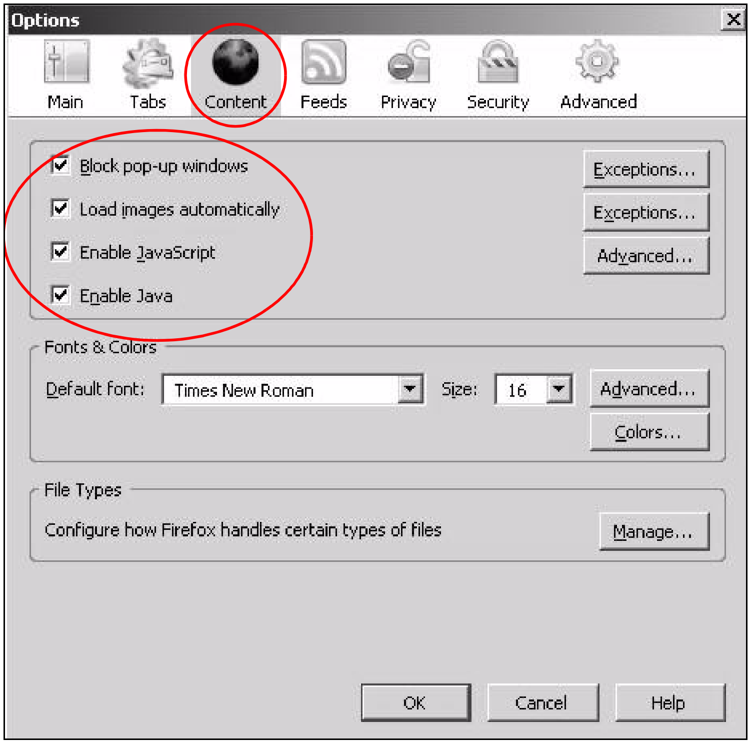
You can enable Java, JavaScript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 169 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 170 Mozilla Firefox Content Security



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Fonts & Colors

Default font: Times New Roman Size: 16

File Types

Configure how Firefox handles certain types of files

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

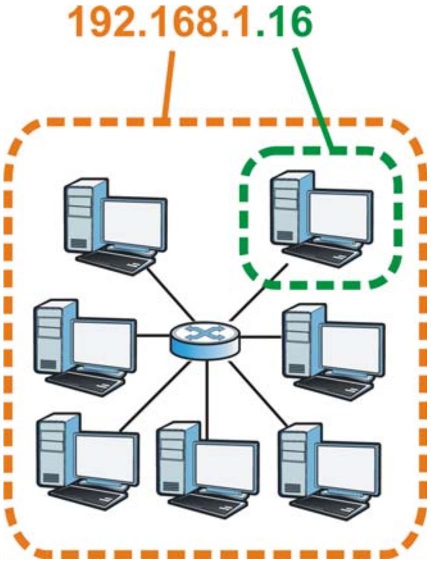
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 171 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 104 Subnet Masks

	1ST OCTET: **(192)**	**2ND OCTET:** **(168)**	**3RD OCTET:** **(1)**	**4TH OCTET** **(2)**
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 105 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 106 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} – 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} – 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} – 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} – 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 107 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

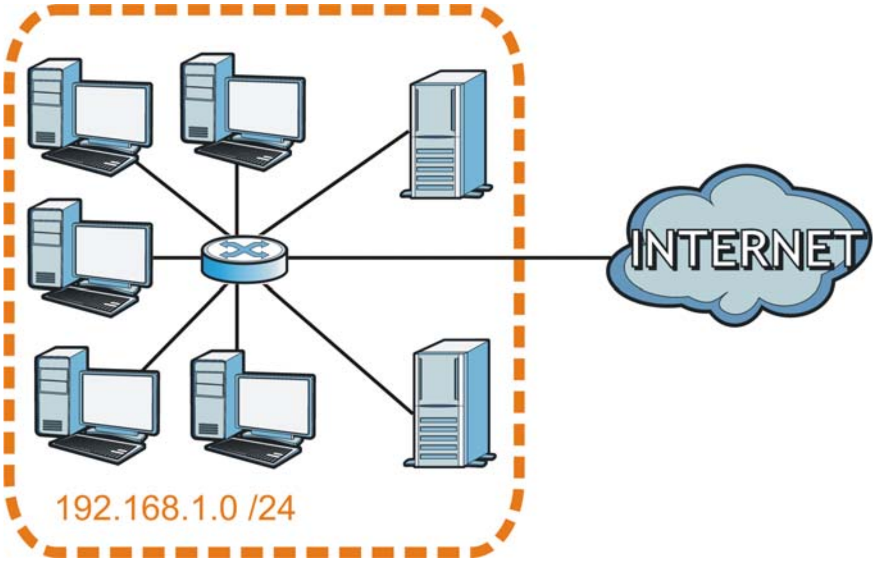
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^8 – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 172 Subnetting Example: Before Subnetting

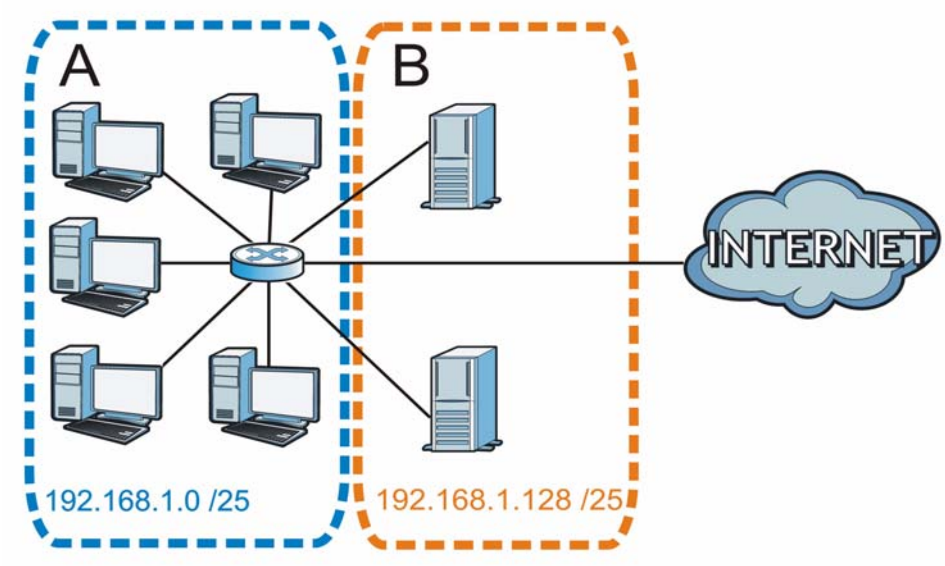


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 173 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of 2^7 – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 108 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 109 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 110 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 111 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 112 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 113 24-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 114 16-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

D

Wireless LANs

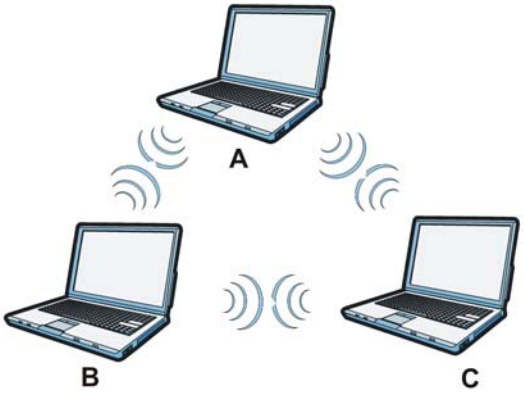
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 174 Peer-to-Peer Communication in an Ad-hoc Network

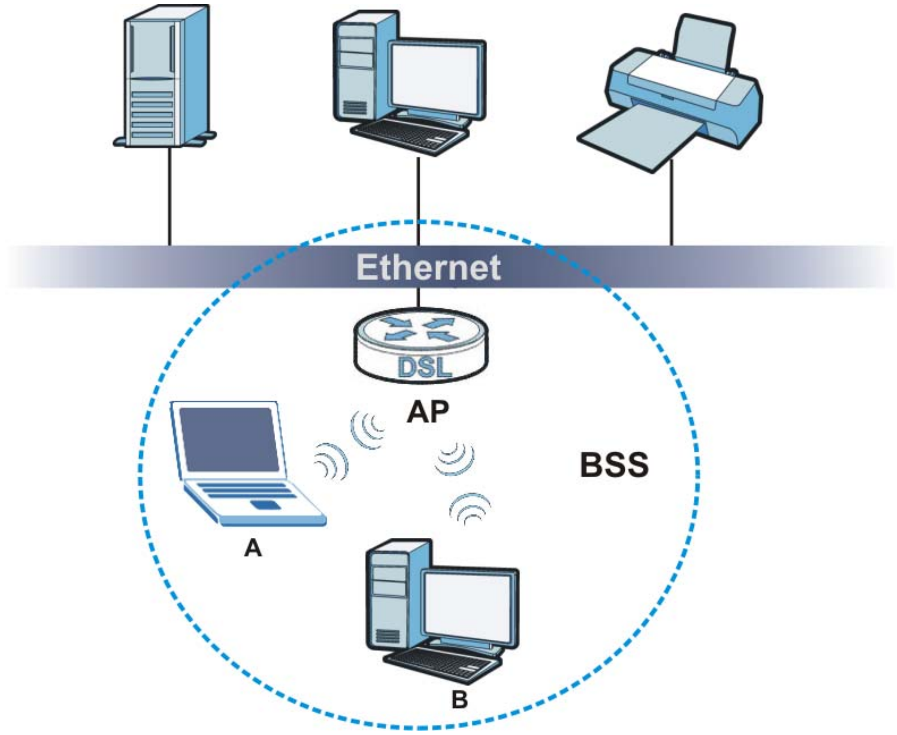


BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 175 Basic Service Set



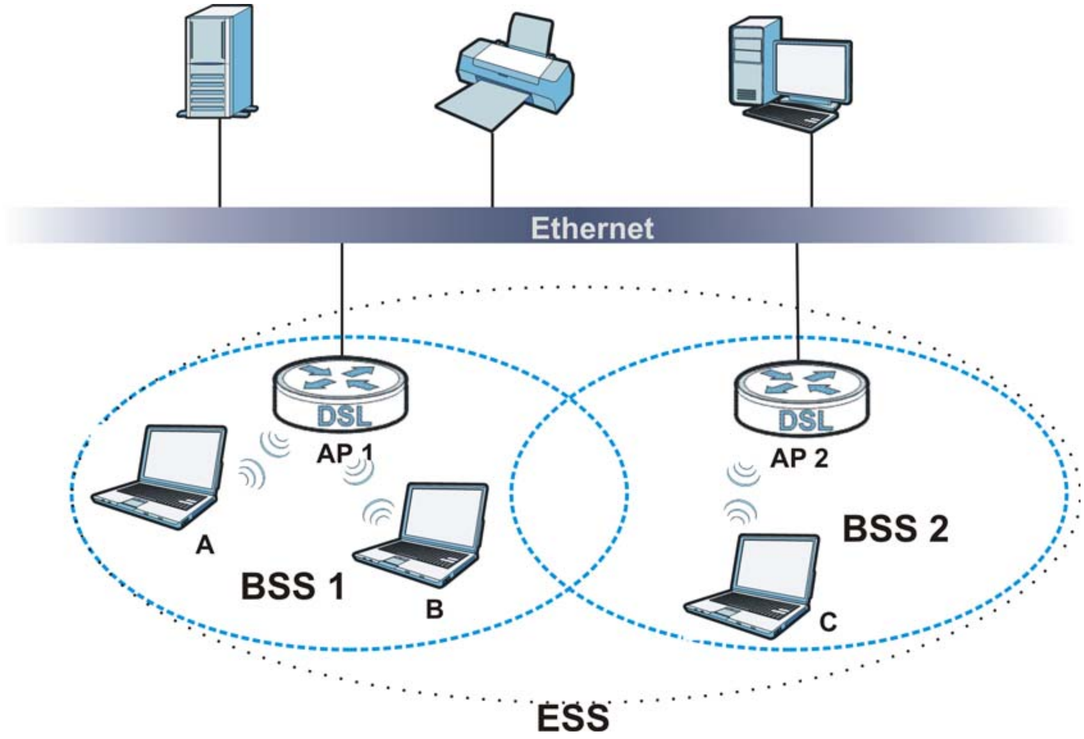
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 176 Infrastructure WLAN



Channel

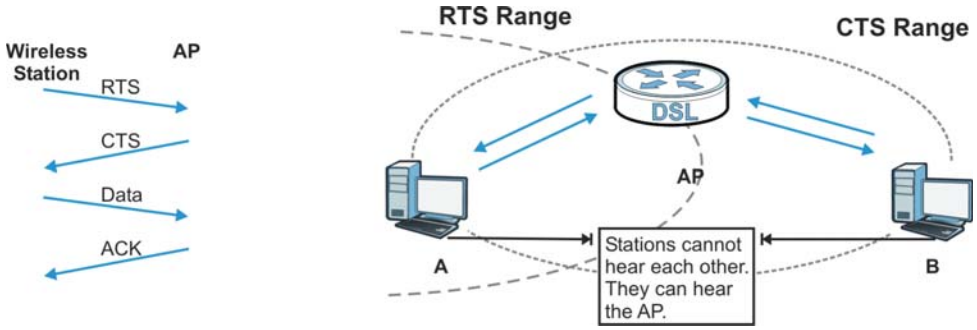
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 177 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 115 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyXEL Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyXEL Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

Table 116 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.

- Authorization

  Determines the network services available to authenticated users once they are connected to the network.

- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.

- Access-Reject

  Sent by a RADIUS server rejecting access.

- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender’s identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-

TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 117 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice. .

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it’s still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

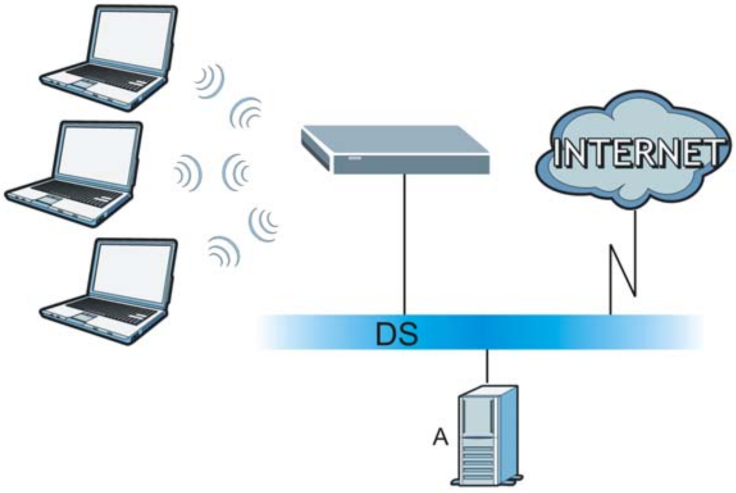
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 178 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

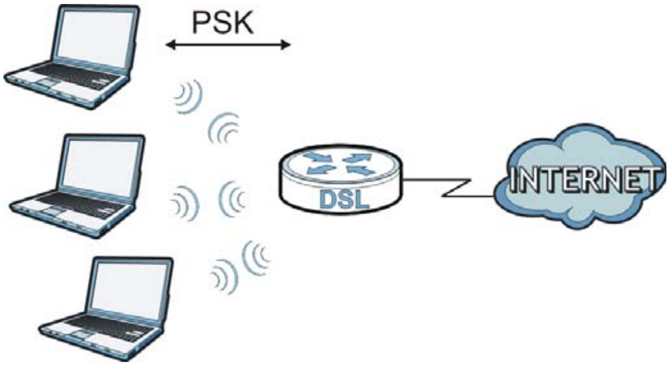
1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 179 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 118 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable

Table 118 Wireless Security Relational Matrix (continued)

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTIO N METHOD	ENTER MANUAL KEY	IEEE 802.1X
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna’s coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

E

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s**) is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 119 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for instance www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.

Table 119 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.

Table 119 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

Open Software Announcements

End-User License Agreement for “P-660HN-51”

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER, CERTAIN ZYXEL’S PRODUCTS MAY CONTAIN–IN PART-SOME THIRD PARTY’S FREE AND OPEN SOFTWARE PROGRAMS WHICH ALLOW YOU TO FREELY COPY, RUN, DISTRIBUTE, MODIFY AND IMPROVE THE SOFTWARE UNDER THE APPLICABLE TERMS OF SUCH THRID PARTY’S LICENSES (“OPEN-SOURCED COMPONENTS”). THE OPEN-SOURCED COMPONENTS ARE LISTED IN THE NOTICE OR APPENDIX BELOW. ZYXEL MAY HAVE DISTRIBUTED TO YOU HARDWARE AND/OR SOFTWARE, OR MADE AVAILABLE FOR ELECTRONIC DOWNLOADS THESE FREE SOFTWARE PROGRAMS OF THRID PARTIES AND YOU ARE LICENSED TO FREELY COPY, MODIFY AND REDISTIBUTE THAT SOFTWARE UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY. NONE OF THE STATEMENTS OR DOCUMENTATION FROM ZYXEL INCLUDING ANY RESTRICTIONS OR CONDITIONS STATED IN THIS END USER LICENSE AGREEMENT SHALL RESTRICT ANY RIGHTS AND LICENSES YOU MAY HAVE WITH RESPECT TO THE OPEN-SOURCED COMPONENTS UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY.

1.Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by international copyright law, trade secret law, international treaty provisions, and the applicable national laws of each respective country. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, you may not market, co-brand, and private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the third party software, and your use of such material is exclusively governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software other than compliance with the applicable license terms of such third party, and makes no warranty (express, implied or statutory) whatsoever with respect thereto. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's TOTAL AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT’S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF

LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan if the parties agree to a binding arbitration. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate free software programs covered under the open source code licenses which allows you to freely copy, modify and redistribute the software. For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (support@zyxel.com.tw), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes MIPS Linux kernel , Bridge-Utils, BusyBox 1.0.0 toolset , Dproxy, ebtables, bftpd, iproute2, iptables, udhcp and zebra software under GPL 2.0 license.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who

places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes ppp software under below license

This directory contains source code and precompiled binaries for ppp-2.4, a package which implements the Point-to-Point Protocol (PPP) to provide Internet connections over serial lines. ppp-2.4 currently supports Linux and Solaris.

All of the code here can be freely used and redistributed. Theindividual source files each have their own copyright and permission

notice; some have a BSD-style notice and some are under the GPL.

This Product includes Ssh server: dropbear software under MIT-style license

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE

AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER

LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,

OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN

THE SOFTWARE.

This Product includes openssl: openSSL library software under BSD-style license

Copyright (c) <YEAR>, <OWNER>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

G

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.

- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 Ghz et/ou 5 Ghz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MhZ.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index

A

ACL rule 159

ACS 231

activation
- firewalls 155
- SIP ALG 144
- SSID 86

Address Resolution Protocol 251

administrator account 259

AH 189

algorithms 189

alternative subnet mask notation 324

antenna
- directional 345
- gain 344
- omni-directional 345

AP (access point) 333

applications, NAT 148

ARP Table 251

ATM
- QoS 76

authentication 98, 100
- RADIUS server 100

Auto Configuration Server, see ACS 231

B

backup
- configuration 267

Basic Service Set, See BSS 331

Basic Service Set, see BSS

broadcast 64

BSS 102, 331
- example 103

C

CA 165, 338

CBR 76

certificate
- details 170
- factory default 166

Certificate Authority
- See CA.

certificates 165
- authentication 165
- CA
- creating 167
- importing 168
- public key 165
- replacing 166
- storage space 166

Certification Authority 165

Certification Authority. see CA

certifications 363
- notices 365
- viewing 365

channel 333
- interference 333

channel, wireless LAN 98

CLI 21

client list 118

Command Line Interface, see CLI

compatibility, WDS 92

configuration
- backup 267
- firewalls 155
- reset 269
- restoring 268
- static route 203, 208, 258

copyright 363

CoS 226

CoS technologies 212

creating certificates 167

CTS (Clear to Send) 334

CTS threshold 95, 98

D

data fragment threshold 95, 98
DDoS 154
default login accounts 259
default server address 143
Denials of Service, see DoS
DH 196
DHCP 114, 129
diagnostic 271
Differentiated Services, see DiffServ 226
Diffie-Hellman key groups 196
DiffServ 226
 marking rule 226
digital IDs 165
disclaimer 363
DMZ 143
DNS 114, 129
Domain Name 148
Domain Name System, see DNS
DoS 154
DS field 226
DS, dee differentiated services
DSCP 226
dynamic DNS 206
 wildcard 207
Dynamic Host Configuration Protocol, see DHCP
dynamic WEP key exchange 339
DYNDNS wildcard 207

E

EAP Authentication 337
ECHO 148
encapsulation 63, 190
 PPPoA 73
 PPPoE 73
encryption 101, 340
ESP 189
ESS 332
Extended Service Set IDentification 80, 88
Extended Service Set, See ESS 332

F

FCC interference statement 363
filters
 MAC address 88, 100
Finger 148
firewalls 153
 add protocols 155
 configuration 155
 DDoS 154
 DoS 154
 LAND attack 154
 Ping of Death 154
 SYN attack 154
firmware 265
 version 37
forwarding ports 134
fragmentation threshold 95, 98, 335
FTP 21, 134, 148

G

General wireless LAN screen 78
guest account 259

H

hidden node 333
HTTP 148

I

IANA 329
 Internet Assigned Numbers Authority
  see IANA
IBSS 331
ID type and content 194
IEEE 802.11g 335
IGA 146
IGMP 64
IKE phases 191

ILA 146
importing certificates 168
Independent Basic Service Set
  See IBSS 331
initialization vector (IV) 340
Inside Global Address, see IGA
inside header 190
Inside Local Address, see ILA
Internet Key Exchange 191
Internet Protocol Security, see IPSec
IP address 64, 74, 114, 130
  ping 271
  private 131
IP alias
  NAT applications 148
IP Sec 177
IPSec 177
  algorithms 189
  architecture 189
  NAT 192
  see also VPN

L

LAN 113
  client list 118
  DHCP 114, 129
  DNS 114, 129
  IP address 114, 116, 130
  MAC address 118
  status 38
  subnet mask 114, 116, 130
LAND attack 154
LEDs 25
limitations
  wireless LAN 102
  WPS 110
Local Area Network, see LAN
login 27
  passwords 28
login account types 259
  administrator 259
  guest 259
logs 245, 253, 261

M

MAC address 89, 118
  filter 88, 100
MAC authentication 88
Mac filter 151
MBS 75
MBSSID 103
multicast 64
  IGMPInternet Group Multicast Protocol, see IGMP
Multiple BSS, see MBSSID
multiplexing 74
  LLC-based 74
  VC-based 74

N

NAT 133, 134, 135, 145, 146, 329
  applications 148
    IP alias 148
  example 147
  global 146
  IGA 146
  ILA 146
  inside 146
  IPSec 192
  local 146
  outside 146
  port forwarding 134
  port number 148
  services 148
  SIP ALG 144
    activation 144
  traversal 193
NAT example 149
negotiation mode 192
Network Address Translation
  see NAT
Network Address Translation, see NAT
Network Map 35
network map 30
NNTP 148

O

OAM Ping Test 272
outside header 190

P

Pairwise Master Key (PMK) 340, 343
passwords 28
PBC 105
PCR 75
Per-Hop Behavior, see PHB 226
PHB 226
PIN, WPS 105
  example 107
Ping of Death 154
Point-to-Point Tunneling Protocol 149
POP3 148
port forwarding 134
PPPoA 73
PPPoE 73
PPTP 149
preamble 96, 98
preamble mode 111
pre-shared key 195
private IP address 131
product registration 366
PSK 341
push button 23
Push Button Configuration, see PBC
push button, WPS 105

Q

QoS 211, 225
  marking 212
  setup 211
  tagging 212
  versus CoS 212
Quality of Service, see QoS

R

RADIUS 336
  message types 337
  messages 337
  shared secret key 337
RADIUS server 100
registration
  product 366
related documentation 3
remote management
  TR-069 231
Remote Procedure Calls, see RPCs 231
reset 26, 269
restart 270
restoring configuration 268
RFC 3164 245
RPPCs 231
RTS (Request To Send) 334
  threshold 333, 334
RTS threshold 95, 98

S

safety warnings 7
SCR 75
secure gateway address 178
security
  wireless LAN 99
security associations, see VPN
Security Log 248
Security Parameter Index 184
Security Parameter Index, see SPI
service access control 163
Service Set 80, 88
Services 148
setup
  firewalls 155
  static route 203, 208, 258
shaping traffic 75
Single Rate Three Color Marker, see srTCM
SIP ALG 144
  activation 144

SMTP 148

SNMP 148

SNMP trap 149

SPI 154, 184

srTCM 228

SSID 100
- activation 86
- MBSSID 103

static route 201
- configuration 203, 208, 258
- example 201

status 35, 39
- firmware version 37
- LAN 38
- WAN 37
- wireless LAN 38

subnet 321

subnet mask 114, 130, 322

subnetting 324

SYN attack 154

syntax conventions 5

syslog
- protocol 245
- severity levels 245

system
- firmware 265
  - version 37
- LED 25
- passwords 28
- reset 26
- status 35
  - LAN 38
  - WAN 37
  - wireless LAN 38
- time 235

T

thresholds
- data fragment 95, 98
- RTS/CTS 95, 98

time 235

TR-069 21, 231
- ACS setup 231
- authentication 232

trademarks 363

traffic shaping 75
- example 75

transport mode 190

trTCM 229

tunnel mode 190

Two Rate Three Color Marker, see trTCM

U

UBR 76

unicast 64

Universal Plug and Play, see UPnP

upgrading firmware 265

UPnP 119
- cautions 115
- example 120
- installation 120
- NAT traversal 114

V

VBR 76

VBR-nRT 76

VBR-RT 76

VCI 74

Virtual Private Network, see VPN

VPI 74

VPN 177
- established in two phases 178
- IPSec 177
- security associations (SA) 178
- see also IKE SA, IPSec SA

W

WAN 63
- ATM QoS 76
- encapsulation 63
- IGMP 64
- IP address 64, 74
- multicast 64

multiplexing 74
status 37
traffic shaping 75
example 75
VCI 74
VPI 74

warranty 365
note 366

WDS 92, 104
compatibility 92
example 104

web configurator 21, 27
login 27
passwords 28

WEP 101

WEP Encryption 82, 83

WEP encryption 81

WEP key 81

Wide Area Network, see WAN

Wi-Fi Protected Access 340

wireless client WPA supplicants 341

Wireless Distribution System, see WDS

wireless LAN 77, 96
authentication 98, 100
BSS 102
example 103
channel 98
encryption 101
example 97
fragmentation threshold 95, 98
limitations 102
MAC address filter 88, 100
MBSSID 103
preamble 96, 98
RADIUS server 100
RTS/CTS threshold 95, 98
security 99
SSID 100
activation 86
status 38
WDS 92, 104
compatibility 92
example 104
WEP 101
WPA 101
WPA-PSK 101
WPS 104, 107
example 109
limitations 110
PIN 105
push button 23, 105

wireless security 335

Wireless tutorial 46

WLAN
interference 333
security parameters 343

WPA 101, 340
key caching 341
pre-authentication 341
user authentication 341
vs WPA-PSK 341
wireless client supplicant 341
with RADIUS application example 342

WPA2 340
user authentication 341
vs WPA2-PSK 341
wireless client supplicant 341
with RADIUS application example 342

WPA2-Pre-Shared Key 340

WPA2-PSK 340, 341
application example 342

WPA-PSK 101, 340, 341
application example 342

WPS 104, 107
example 109
limitations 110
PIN 105
example 107
push button 23, 105